NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

POLICY AND POLICY FORMULATION CONSIDERATIONS FOR INCORPORATION OF SECURE MOBILE DEVICES IN USMC GROUND COMBAT UNITS

by

Robert J. Epstein

September 2014

Thesis Advisor: Nancy Roberts
Second Reader: William Robinette

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2014	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE POLICY AND POLICY FORMULATION CONSIDERATIONS FOR INCORPORATION OF SECURE MOBILE DEVICES IN USMC GROUND COMBAT UNITS			**5. FUNDING NUMBERS**
6. AUTHOR(S) Robert J. Epstein			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

Modern information technology evolves at a rapid pace, and the U.S. Marine Corps ground combat units require cutting-edge capabilities in order to maintain a competitive advantage. The advent and military application of smartphones and smartphone applications provide a plethora of advantages that these forces seek to leverage, yet the very rapidity of their development presents a host of network security problems.

This thesis examines the conceptual risk framework for incorporating smartphones into ground combat units, and uses a cutting-edge smartphone capability, the Field Information Support Tool, as a case study. Furthermore, the comparatively slow policy-making process of the DOD ensures that policy requirements will lag behind the emerging technologies and the novel threats these technologies introduce. This thesis conducts a policy review of existing DOD policies that apply to smartphones and network security, as well as examines and models the policy formulation process in an effort to reform it in a way more conducive to the incorporation of fast-growing capabilities.

14. SUBJECT TERMS smartphones, mobile device management, Field Information Support Tool, change management, business process reengineering, design thinking, knowledge value added.			**15. NUMBER OF PAGES** 155
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

POLICY AND POLICY FORMULATION CONSIDERATIONS FOR INCORPORATION OF SECURE MOBILE DEVICES IN USMC GROUND COMBAT UNITS

Robert J. Epstein
Captain, United States Marine Corps
B.S., United States Naval Academy, 2008

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2014

Author: Robert J. Epstein

Approved by: Nancy Roberts
Thesis Advisor

William Robinette
Second Reader

Dan Boger
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Modern information technology evolves at a rapid pace, and the U.S. Marine Corps ground combat units require cutting-edge capabilities in order to maintain a competitive advantage. The advent and military application of smartphones and smartphone applications provide a plethora of advantages that these forces seek to leverage, yet the very rapidity of their development presents a host of network security problems.

This thesis examines the conceptual risk framework for incorporating smartphones into ground combat units, and uses a cutting-edge smartphone capability, the Field Information Support Tool, as a case study. Furthermore, the comparatively slow policy-making process of the DOD ensures that policy requirements will lag behind the emerging technologies and the novel threats these technologies introduce. This thesis conducts a policy review of existing DOD policies that apply to smartphones and network security, as well as examines and models the policy formulation process in an effort to reform it in a way more conducive to the incorporation of fast-growing capabilities.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

3G	third generation
4G	fourth generation
APAN	All Partners Access Network
ASD (NII)	Assistant Secretary of Defense for Networks & Information Integration
BAT	Biometric Automated Toolset
BPR	business process reengineering
BYOD	bring your own device
C4	command, control, communications, and computers
CAC	common access card
CIO	Chief Information Officer
COI	community of interest
COIN	counterinsurgency
CORE	Common Operational Research Environment
COTS	commercial-off-the-shelf
CPI	continuous process improvement
CPOF	Command Post of the Future
CPS	Certificate Practice Statement
DCGS	Distributed Common Ground System
DISA	Defense Information Systems Agency
DISR	DOD IT Standards Registry
DOD	Department of Defense
DODD	Department of Defense directive
DODI	Department of Defense instruction
DON	Department of the Navy

DOPSR	Defense Office of Publication and Security Review
DT&E	developmental testing and evaluation
FIST	Field Information Support Tool
GFE	government furnished equipment
HIIDE	Handheld Interagency Identity Detection Equipment
HQMC	Headquarters Marine Corps
IE	information enterprise
IT	information technology
JBC-P	Joint Battle Command-Platform
JOLTED TACTICS	Joint Operational Long Term Evolution Deployable Tactical Cellular System
LTE	long-term evolution
KVA	knowledge value added
MARCORSYSCOM	Marine Corps Systems Command
MCEN	Marine Corps Enterprise Network
MCIENT	Marine Corps Information Enterprise
MDM	mobile device management
NIPRNET	Non-classified Internet Protocol Router Network
NPS	Naval Postgraduate School
NSA	National Security Agency
NSS	national security systems
OGC	Office of the General Council
OS	operating system
OSD	Office of the Secretary of Defense
OTM	on the move
OT&E	operational testing and evaluation
PED	personal electronic devices
PK	public key

PKI	public key infrastructure
POA&M	plan of action and milestones
RMF	risk management framework
ROK	return on knowledge
SecDef	Secretary of Defense
SEEK	Secure Electronic Enrollment Kit
SIPRNET	Secure Internet Protocol Router Network
SMC	secure mobile cellular
SMF	secure mobile framework
TANG	Tactical Advancements for the Next Generation
TIGR	Tactical Ground Reporting System
TQM	total quality management
UCAPL	Unified Capabilities Approved Products List
USMC	United Stated Marine Corps
USSOCOM	U.S. Special Operations Command

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my thesis advisor, Dr. Nancy Roberts, and second reader, CDR William Robinette, USN, for their guidance and assistance throughout the thesis process. I would also like to thank Headquarters Marine Corps C4 Command, Control, Communications, and Computers for its cooperation and responsiveness as I sought information for my study.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

While commanding the U.S. Army's Training and Doctrine Command (TRADOC) from December 2008–March 2011, Chairman of the Joint Chiefs of Staff, General Martin Dempsey eloquently stated, "With the introduction of the iPhone and the 3G network, access to information all-the-time exploded. The question for us is whether we're going to ignore it, or seek to take advantage of it" (Grindle, 2011, p. 1). In the intervening years, the Department of Defense (DOD) has sought to capitalize on the ubiquity of smartphone technologies and the corresponding familiarity modern service members have with them to improve garrison and deployed operations. Simental (2010) explained that "the Army wants to employ…everyday smartphone technology tools…in garrison…and, eventually, in combat operations" (p. 20). Current programs, such as the Joint Battle Command-Platform (JBC-P), fielded by the U.S. Army and U.S. Marine Corps (USMC) forces starting in fiscal year 2013 (FY13), are designed to upgrade current Blue Force Tracker (BFT) applications as well as introduce a suite of Android-based smartphone applications for tactical operations. The JBC-P will come with a standard set of mapping, Global Positioning System (GPS) enabled BFT and Tactical Ground Reporting graphics and critical messaging (Heininger, 2011). Indeed, as the JBC-P program attests, smartphones have become much more than mere communication devices. Modern smartphones are more akin to hand-held mobile computers with the potential to provide real-time information and intelligence in a combat environment. This capability implies the inherent need for passing classified information and incurs all the risks entailed in transmitting classified military information.

While the Army is leading the smartphone effort, the USMC has also taken note of the potential uses of smartphones, authorizing recruiters to use phones to take photos of prospective recruits (Sanborn, 2011). More telling is the USMC-Lockheed Martin initiative to provide a tactical Smartphone network in support of Humanitarian Assistance and Disaster Relief (HADR) missions (PR Newswire, 2011). The system, named MONAX, provides a portable fourth generation (4G) private cellular network for off-the-

shelf smartphones with voice, data, and video services. Though constructed primarily for HADR, the utility implications for smartphone apps across a broad range of military operations, to include combat reporting and intelligence dissemination, is self-evident. When viewed together, the JBC-P, Army outlook, and USMC initiatives evince the DOD's push toward smartphone technologies and uses, and that these applications are here to stay.

Despite the smartphone-driven explosion of wireless and cellular-enabled web-access in the private sector, the military has been relatively slow to adopt the smartphone wholesale as programs of record. As a result of the reactive nature of DOD's approach, and particularly that of the USMC, which has heretofore allowed the Army to do most of the heavy lifting regarding smartphone technology development, security considerations and policy creation regarding the use of classified smartphone capabilities at the tactical level remain largely ignored. In what appears to be an interim solution, the Army has turned to dealing with security of smartphones in much the same manner as computers and other mobile devices (Kenyon, 2011). Specifically, the governing policy remains the DOD Directive (DODD) 8100.02 (2004), which is the "use of commercial Wireless Devices, Services, and Technologies in the Department of Defense Global Information Grid." Additionally, the Army has tried to conform to the DODD 8100.02 by incorporating the use of common access card (CAC) public key infrastructure (PKI) capabilities. While this analogy approach is a useful starting point, treating a classified smartphone as any desktop computer overlooks some of the very aspects that make it such an attractive item; it's light, hand-held mobility, ubiquity, tailored application modularity, small logistical footprint, and constant connectivity to the World Wide Web. The USMC, lagging behind the Army in smartphone implementation and even further in policy development, has yet to formulate policy beyond the published DODD 8100.02. As such, an in-depth policy and policy creation process review is warranted to ensure prudent policy formulation keeps pace with the security risks posed by wholesale adoption and incorporation of classified smartphone technologies within tactical USMC ground combat units, but which also expedites needed capabilities into the hands of the warfighters who require them to accomplish their critical missions.

B. PROBLEM STATEMENT

The current USMC processes for crafting security policy are too slow and unresponsive compared to the rapidly advancing field of cellular mobile smartphone communication technologies. As a result, there is a dearth of proper security policies for incorporating these technologies into U.S. Marine Corps operational ground combat units despite warfighters' calls for their adoption. In addition, a lack of sufficient security policy and unresponsive and ill-suited policy formulation process results in costly delays fielding asked-for tools to the end-user, and increased costs associated with reworking legacy systems to accommodate security threats. Furthermore this mismatch has the potential to result in compromise or spillage of classified material as smartphone technologies and capabilities appear in and are used by operational forces in both garrison and deployed environments absent judicious guidance or regulation.

C. PURPOSE STATEMENT

The purpose of this research is to propose recommendations for future security policy and policy creation processes in order to decrease the costly lag time between technological development and adoption and the security policies access to DOD networks and end-user privileges. The expressed objective of this research is to propose a framework for a more responsive IT system policy formulation process as well as to provide policy guidance, based on the proposed framework, for incorporating the Field Information Support Tool's (FIST) smartphone technologies into operational USMC ground combat units. Moreover, while this research will be conducted primarily with regards to U.S. Marine Corps policy and policy formulation processes, the recommendations will likely apply across the defense establishment, and could be used to improve security policy and process for mobile cellular smartphone technologies DOD-wide.

D. RESEARCH QUESTIONS

1. What is current policy regarding hand-held mobile smartphone technologies?

2. What are the issues concerning this technology?

3. What policy changes must the Marine Corps make to take advantage of smartphone technology?

E. RESEARCH METHODS

This research relies on archival research and software simulation. No field or laboratory testing is required. The primary sources for this thesis are existing security policies in the DOD, component service branches (Army, Navy, Air Force, Marines), and other federal agencies. The FIST project at the Naval Postgraduate School is used as a backdrop and case study example of a smartphone-based information technology system whose incorporation into the operational forces suffers from the limitations of the policy creation process. In order to assess the current policy formulation process, Savvion Process modeling software will be used to map and model the current (As-Is) process as well as a possible future (To-Be) process for comparison and analysis. This method will ensure the maintenance of a practical focus to the research as well as allow for the creation of recommended policy to govern incorporation smartphone-enabled capabilities into USMC ground combat units.

F. DATA, OBSERVATION, AND ANALYSIS METHODS

The method of analysis for this thesis will be a literature review of security policies governing other information communication technologies and those concerning cellular technologies, a study of the FIST/Lighthouse programs at the Naval Postgraduate School to provide a conceptual background to highlight the impact of existing and recommended policies, and a simulation of the current DOD policy formulation process using the Savvion business process modeling tool.

G. POTENTIAL BENEFITS AND LIMITATIONS

This study could identify serious gaps in current U.S. Marine Corps policy concerning incorporation of classified smart-phone technologies into the operating forces. The identification of these gaps, in conjunction with a set of recommendations for future policy formulation, would allow the USMC the opportunity to revise and create security policies concurrent and concordant with technological development, and in advance of

system procurement. Ultimately, the ability to set educated policy into place early will prevent classified material compromise stemming from insufficient security policies or protocols, reduce system re-work costs to meet reactive and retroactive policy, and allow for timely incorporation of capabilities into the operating forces. Lastly, the introduction of proper policy concurrent with technology development ensures minimization of cost-overruns and system delays resulting from failure to conform to required standards.

This research will be limited in its scope due to the overall classification level of the final product. A SECRET and/or TOP-SECRET study would be required in order to provide a more comprehensive assessment of vulnerabilities to the existing technology.

H. ORGANIZATION OF THE THESIS

This research is organized into seven chapters. The first chapter provides an introduction the research topic area, outlines the problem space, the research's purpose statement, the questions the research will seek to answer, and the methods by which the research will attempt to answer them.

The second chapter provides a literature review of the technological capabilities of smartphones, vulnerabilities inherent in their use, uses of smartphone for tactical USMC ground combat units, and ways to implement mobile devices into these units. The second chapter also provides a review of existing top-level DOD and USMC policies concerning mobile devices as well as a policy review of DOD security policies.

The third chapter provides an overview of the FIST system, identifies issues arising from its introduction, implementation, and use, and provides an analysis of the gaps between existing security policies and the vulnerabilities of the FIST system as a case study for the larger gap between mobile device security and policy. This chapter also presents a series of specific recommendations for bringing current security policy in line with the vulnerabilities in the FIST system.

The fourth chapter details the simulation methodology and presents how the process was transcribed from the DOD Issuances website and into the Savvion process modeler. This chapter then goes further to present a simulation of a proposed future (To-

Be) policy formulation process based upon the ideas of business process reengineering and Design Thinking, again using the Savvion process modeler.

The fifth chapter presents and compares the data and results from the simulations run as part of chapter four.

The sixth chapter comprises an analysis of the results from the simulations, described in chapter five, and a discussion of how such a change effort might be managed in light of the interrelated fields of business process reengineering, change management, and Design.

The seventh chapter summarizes the scope and organization of the research, provides conclusions about the results of the research, and outlines suggested areas for future research.

II. LITERATURE REVIEW

This chapter provides a review of the technological capabilities of smartphones, vulnerabilities inherent in their use, and ways to implement mobile devices into tactical USMC ground combat units. This chapter also reviews existing top-level DOD and USMC policies concerning mobile devices as well as DOD security policies.

A. TECHNOLOGY OVERVIEW

1. Technological Capabilities

What people enjoy most about smartphones is their utility as an all-purpose communication and information-accessing device in the palm of one's hand. As such, the smartphone includes many features and characteristics not commonly associated with classified desktop/laptop computers such as open-source internet and email access, geo-tagging features, the necessity for existing wireless and cellular networks, and ease of loss of such a small device. Thus, pushing classified material wirelessly to a potentially unsecured smartphone inherently puts the Secure Internet Protocol Router Network (SIPRNet) at risk (Bacon, 2011). This risk only increases in light of excitement over the morale, welfare, and recreation (MWR) uses for smartphones in a deployed environment. Mixing the ability to read biometric data about suspected insurgents with the notion of using smartphones to keep personnel stationed at austere and remote forward operating bases (FOB) connected with family and friends via social media poses worrisome concerns about operational security (OPSEC) and compromise of classified material (Simental, 2010).

The problems surrounding securing computers and computer networks in the internet age are hardly new. Thus, as outlined in the DODD 8100.02 (2004), enforcing CAC-enabled PKI is indeed a viable method for ensuring user authenticity and non-repudiation. However, the challenge is moving from the practical means of solving computer security issues to the unique challenges of the tactical environment (Bacon, 2011). Current Army policy requires smartphones to receive a Certificate of Networthiness from the Army Enterprise Designated Approval Authority prior to

connecting to Army networks and their inclusion on the DOD Unified Capabilities Approved Products List (UC APL), which attests to a device's interoperability and information assurance accreditation (Kenyon, 2011). While the enactment of these policies in the Army is certainly more aggressive than in the USMC, which has yet to write initial policy, treating the smartphone as just another computer with access to the network, to say nothing of a classified network, fails to take into account several fundamental differences between the two. The USMC must reevaluate the ways in which it creates policy for information technologies in order to ensure the user requirements are satisfied while also protecting access to classified networks through sensible standards, guidelines, and regulation.

2. Technological Vulnerabilities of Smartphones

a. Loss or Theft of the Device

As VanAssche (2014) asserted, the primary difference between security for traditional computer and network systems and smartphones and other mobile devices is the inherent difficulty of safeguarding the physical security of the devices, as they are, by definition, designed to be highly portable. Such portability represents a significant security threat, as one of the primary assumptions in most computer and network security planning entails that the physical security of the systems will remain intact. The integrity of the system leads to the follow on assumption that the potential attacker will have to access data and systems via some external attack avenue, rather than from inside the system itself (Simpson, Backman, & Corley, 2011).

Another important consideration is that mobile device security risks are not limited to accidental loss or theft. Improper disposal or turnover of mobile devices also presents a significant threat (VanAssche, 2014). Failure to completely remove sensitive information from devices prior to disposal affords access to a rich information store contained within the device itself, regardless of if that device retains access to the original systems (Landman, 2010). Worse yet, if the device continues to have access to its original systems, improper disposal of the device fundamentally negates the implemented

and planned security measures, and compromises the system's integrity in a way that is extremely difficult to detect or prevent (Seth & Keshav, 2005).

b. Security Risks of Smartphone Platforms

Moving away from the security risks introduced by the loss or theft of mobile devices and the subsequent and serious exploitation potential incurred due to an attacker's possession of the device, the characteristics of the mobile devices' platforms add security risks, as well (VanAssche, 2014). As Ahmed and Ahamad (2012) suggested, flaws in platform security architecture produce two security threats. First is the ability of an external attacker to access the device's data while foregoing authentication or identity verification. Second is the device's ability to access systems based off of the trust inherent in possession of the device and using the device as an authentication criterion.

In order to prevent exploitation based off of the security threats identified above, designers must take care to evaluate the security implementation of the mobile device itself. This evaluation of the device's operating system and architecture should be based off of key characteristics identified by Zefferer, Kreuzhuber, and Teufl (2013) as follows:

> *Access protection*: This aspect covers the platform's support for access protection features. These features assure that only legitimate users are able to access the smartphone's GUI and data stored on the device. Typical implementations of access-protection mechanisms on smartphones rely on password based authentication schemes. When assessing the security of a smartphone platform, the set of supported access-protection methods and their resistance against known attacks need to be considered.
>
> *Encryption*: Encryption is a cryptographic method that assures the confidentiality of data. Current smartphone platforms typically support different types and methods of encryption. An important aspect of encryption systems is the secure derivation and storage of encryption keys that are used to encrypt confidential data. The set of supported encryption methods and implemented key-derivation functions are hence main aspects that need to be considered when assessing the security of smartphone platforms.
>
> *Secure storage of credentials*: PINs, passwords, or cryptographic keys that grant access to protected data or services are usually subsumed under the term credentials. Credentials represent highly confidential data that need

> to be appropriately protected when being stored on smartphones. Some smartphone platforms provide especially protected storage locations for credentials. The availability of such storage locations and their capability to protect credentials are important aspects that need to be considered when assessing the security of smartphone platforms.
>
> *Mobile device management*: Supported security features such as access protection or encryption are typically optional and need to be manually enabled by the user. Experience has shown that users often refrain from activating these features for convenience reasons. Mobile device management (MDM) has recently evolved as a potential solution to this problem, as it allows for a central management and configuration of smartphones. Furthermore, MDM allows for remote execution of tasks and routines on smartphones. This way, data stored on smartphones can for instance be remotely deleted (remote wipe) when the device gets lost or stolen. (pp. 129–130)

Since shortfalls or deficiency in any one, or more, of these key areas represents a serious security risk, a platform must successfully and comprehensively address each of these four areas to be considered a secure mobile platform (VanAssche, 2014).

Addressing the second security threat depends on the authentication method the system uses to verify that a user is valid, and not in violation of confidentiality protections, prior to allowing access to a system or data (VanAssche, 2014). Ahmed and Ahamad (2012) asserted that any system or application which relies solely, or primarily, on possession or capabilities of the mobile device alone (for instance, using a device serial number or some other intrinsic identification method), cannot be considered reliably secure. Rather, in order to maintain confidentiality protections, the user must provide some form of authentication that is unique to that user, and entirely separate from the device (VanAssche, 2014). Ideally, this authentication system would be based on identical criteria as non-mobile platform authentication. Unfortunately, as Varadharajan (2000) argued, identical methods are not always possible, such as in cases where mobile devices do not support common structures such as physical access tokens (i.e., smart cards/CAC). Such instances require system architects and security designers to recognize the disparity and to institute equivalent authentication procedures in order to maintain comparable levels of security within the system (VanAssche, 2014).

c. Risks in the Supporting Architecture

Though a detailed discussion of the risks to the technological architecture which supports mobile devices is beyond the scope of this research, it is sufficient to say that the back-end systems such as the server and data transport are also at risk. Elucidation of these risks falls within the realm of computer security, and encompass a whole new series of complicated protocols and governing policies.

3. Vulnerabilities Stemming from Smartphone Usage

It is the very dual use potential of smartphones, for both personal and business functions, which makes them both an attractive platform and a security risk (Hibbard, 2011). In essence, the armed services must balance the smartphone's power as an information accessing and social media tool with the necessarily restrictive nature of access to classified material. The USMC must therefore treat the viruses and malware affecting smartphones as it would those attacking any other information system (Hibbard, 2011). The deceivingly simple answer to this problem is that unit-level information technology (IT) professionals need to implement security measures to protect smartphones from worms, viruses, and Peer-to-Peer applications (Hibbard, 2011). However, absent unified security policy from the DOD or Headquarters Marine Corps, these measures would be recommendations only, and subject to change or allowed to lax during the frequent personnel rotations which characterize the DOD.

Current research or policy does not discuss or evaluate the social engineering and counterintelligence risks posed by smartphone interaction with social media sites, and yet, as this is one of the primary uses of the smartphones which leadership foresees, a security policy review taking these factors into account is critical. Smartphones contain more personal data than was stored in older, analog phones (Eaton, 2010). Smartphones have numerous applications that store critical and sensitive information such as login names and passwords, contacts, or other identifying information that an adversary could use to re-create sensitive information (Hibbard, 2011). For example, currently, the government-issued BlackBerrys have automated links to the workplace and email, which, in turn, means that a lost phone could jeopardize all of the sensitive information located

in e-mail, contacts, social networking applications, and geotagging. Geotagging, the process of adding geographical identification to photographs, video, websites, and SMS messages, is one of the greatest threats to social networking sites, and by extension, smartphones with enabled social networking features (Robillard, 2011). Geotags embed the equivalent of a 10-digit grid coordinate in pictures taken with smartphones. When that picture, video, or message posts to the Internet, key personal or operational information is provided to the world, and by consequence, to the enemy (U.S. Army Office of the Chief of Public Affairs, 2011). Location-based social networking is growing in popularity and increasing the military's OPSEC threat. These applications, ubiquitous on smartphones, are extremely dangerous, and easily interpreted by adversaries. Location-based social networking helps adversaries establish patterns, exposes places of duty and home station by tracking movements, and aggregating information that identifies locations of service personnel (U.S. Army Office of the Chief of Public Affairs, 2011). While it is easy to stipulate that the solution lies simply in having leadership educate and mandate personnel to disable geotagging in smartphones or forbid posting geotagged media to social media sites, the very existence of the capability in the hands of deployed personnel increases the likelihood of spillage (U.S. Army Social Media Handbook, 2011, p. 5). Despite guidance concerning geotagging within the Army, there currently exists no codified security policy within the DOD or the USMC to address geotagging security concerns at the tactical ground combat unit level when the compromise of such information can spell mission failure.

As Hibbard (2011) attested, worse than information found within geo-tagged pictures, real time location tracking of soldiers or Marines both in the continental United States and abroad also poses a significant threat. What Hibbard's (2011) study does not address is how this vulnerability is exacerbated when facing a technologically savvy foe, or in remote areas such as Afghanistan where infrastructure is limited, and ad-hoc networks are required to be established. There are three basic techniques to determine the location of a cell phone or other similar device: using GPS, cell phone tower triangulation, and tracking Wi-Fi signals from transmitters (Privacy Rights Clearinghouse, 2011). While such real-time location tracking, as is currently found in

Blue Force Tracker, is a useful tool for ground commanders, the way in which smartphones perform this function through Wi-Fi signals and cell phone towers opens up the ground combat force to exploitation by the enemy, which can use the technology in much the same manner to determine friendly locations. While the capability is known, as well as the self-evident damage should the enemy acquire such information, there currently exists no codified security policy within the DOD or the USMC to address these triangulation concerns at the tactical ground combat unit level.

Commercial-off-the-shelf (COTS) technologies carry the added vulnerabilities that the DOD has little to no control over their manufacture. Of particular note is the fact that these devices and their associated software might be developed in foreign countries which, while their economic interests might align compatibly with those of the United States, might wish to degrade or have access to U.S. foreign policy and military capability. Put more simply, it is not above a modern nation state to introduce malicious software into COTS systems in order to gain a national advantage. For instance, a government could, and indeed has, insert a

> "sleeper" program that embeds in [a victim's] computer. That program can be controlled remotely, allowing the attacker to access e-mail, send confidential documents to a specific address—even turn on a Web camera or microphone to record what is going on in the room. In many cases, a user does not know he has been the victim of an attack. (Cha & Nakashima, 2010, p. 2)

Despite the vulnerabilities, the pervasiveness and reliance on smartphones means that in conjunction with the absence of existing policy, ground combat units will continue to search for a way to satisfy their need for a mobile, hand-held field data-collection and analysis system. Based up on service culture, organizations are likely to proceed in one of two ways. Either they will say that unless allowed by regulation, such technologies are forbidden, or they will take the opposite approach and use technologies unless prohibited by order and regulation. Take, for example, the following testimony from two Marine captains who recently served in Iraq and Afghanistan:

> During a recent deployment to Afghanistan in support of Operation Enduring Freedom (OEF), the officer had several experiences with regards to cellular devices. As a logistician for a Special Operations Task Force

(SOTF), the officer filled an information sharing gap by purchasing cellular devices through the local Afghan market. The "flip phones" and "blackberries" used Afghan minute cards which were also bought through the local market. The phones operated on the existing Afghan network. These cellular devices were issued to key personnel throughout the support center. In total there were approximately 40–60 cellular devices that were either turned over from redeploying SOTF personnel or bought for the support center of 150 Marines. Marines who did not receive a turned over or issued cellular device bought their own through the local market.

These cellular devices proved to be a valuable piece of Command and Control (C2) not only for the officer within the support center, but also supporting the Special Operations Teams throughout the country. Specific examples were the ability to enhance multi-tasking, find personnel more easily, speed up support, and pass information more effectively. Since the devices used were not encrypted, the type of information sharing was limited, but still allowed for better logistics support throughout the battalion, a wider distribution of personnel and faster flow of information up and down the chain of command.

One specific example was an issue with a particular air re-supply drop. Each Special Operation Team also had a local Afghan cellular capability. Able to use the cellular device in a limited capacity, the officer was able to contact the remote Team and adjust the re-supply given a time sensitive situation. Another observation on the use of cellular devices was noted during a visit to Camp Leatherneck, Afghanistan. The officer observed many of the Marines possessed personal Afghan cellular devices in and around the camp using both voice and text capabilities. Upon asking the Marines how they were using the devices; it became clear they were organizing and passing information much like they would in a garrison environment. These observations and experience in a fast-paced tactical environment posed the question, "Why doesn't the Marine Corps have cellular or smartphone devices for Marines operating at the tactical edge?" This same question was posed to the officer at a remote site in Afghanistan by a Staff Sergeant who simply asked, "Why can't we have a mobile network to use secure cellular smartphones?" This question highlights the perceived technology gap between the information agility the Marine wanted and what was available. These needs and actions observed while deployed spawns the idea to have government issued smart devices that can communicate voice, text and data; enhancing information flow up and down the chain of command. Leveraging commercial off the shelf technology has the potential for the Marine Corps to increase capabilities, decrease logistics support which in turns provides cost savings. Marines buying these phones on their own accord demonstrate a certain willingness to pay (WTP). (Liguori & Daniel, 2013, pp. 1–2)

As can be seen clearly in the anecdote above, Marines will find a way to get their mission accomplished, to include using devices whose network security and authorization lie in gray areas on the peripheries of current accepted platforms. On the other hand, the questions posed above are perfectly legitimate given the pace, scope, and capability of modern cellular communications technology. The ambiguity and lack of policy and a responsive policy crafting process introduces unnecessary risk of classified material that can compromise warfighters whose missions—and lives—depend on having information in the palms of their hands. A review of the existing literature demonstrates the policy to be insufficient and illustrates that the creation process is unresponsive. This research intends to carry the effort forward and propose a framework for a more responsive IT system policy formulation process as well as provide policy guidance, based off of the proposed framework, for incorporating smartphone technologies into operational USMC ground combat units.

4. Ways to Implement Secure Mobile Cellular into Tactical Units

The following section discusses several alternatives for achieving secure mobile cellular (SMC) capabilities in ground combat units using emerging technologies. This section is useful since it serves to link the smartphone application and backend server discussion from Lighthouse/FIST with the capabilities to enable such a system in a deployed environment. In other words, reliance on a previously established cellular infrastructure is not inherently necessary to operate a SMC network.

a. Lockheed Martin's MONAX System

The MONAX system, developed by Lockheed Martin, is a private, deployable, cellular network which provides 3G and 4G communications capabilities to low-cost, commercially available, Wi-Fi-enabled devices (IS&GS Defense, n.d.). The MONAX system delivers secure multimedia Internet protocol (IP) services such as voice, data, and video to mobile users (IS&GS Defense, n.d.). The MONAX system consists of a sleeve, called the Lynx, as well as a base station. The base station can be either single sector or three sectors (a sector is a 120-degree transmission/reception swath achieved using a directional antenna). Three sectors provide 360 degrees of coverage. MONAX base

stations may be operated in fixed configurations or mounted on vehicles for OTM communications. As depicted in Figure 1, MONAX is a rapidly deployable tactical cellular system which can be operated from a fixed or mobile platform and which aims to provide support to the individual user and mobile user (IS&GS Defense, n.d.).

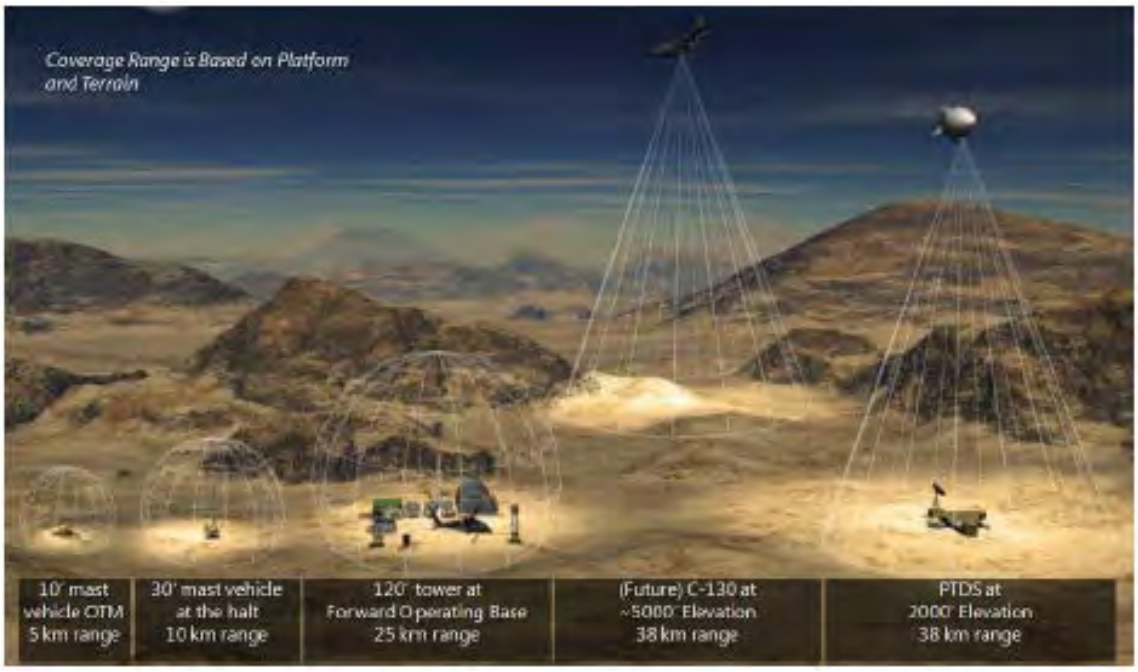

Figure 1. Lockheed Martin MONAX Concept of Operations (from IS&GS Defense, n.d.)

b. Oceus Networks' Xiphos System

In a program named Joint Operational Long Term Evolution Deployable (JOLTED)—Tactical Cellular System (TACTICS) Joint Capabilities Technical Demonstration (JCTD), the U.S. Army has also sought to implement and benefit from COTS technology. JOLTED-TACTICS provides robust communications to dismounted, fixed or OTM tactical users through its COTS-Internet Protocol (IP)-based system (Whittaker, 2011). This system employs innovations in fourth generation (4G) long-term evolution (LTE) cellular technologies to deliver data rates on the order of Megabits to mobile and dismounted users equipped with smartphones or other personal electronic devices (PED) (Liguori & Daniel, 2013). As Figure 2 shows, through the use of

JOLTED-TACTICS, tactical units are able to access applications such as streaming media, Voice over Internet Protocol, e-mail, and instant messaging for immediate situational awareness using COTS 4G/LTE technologies (Whittaker, 2011).

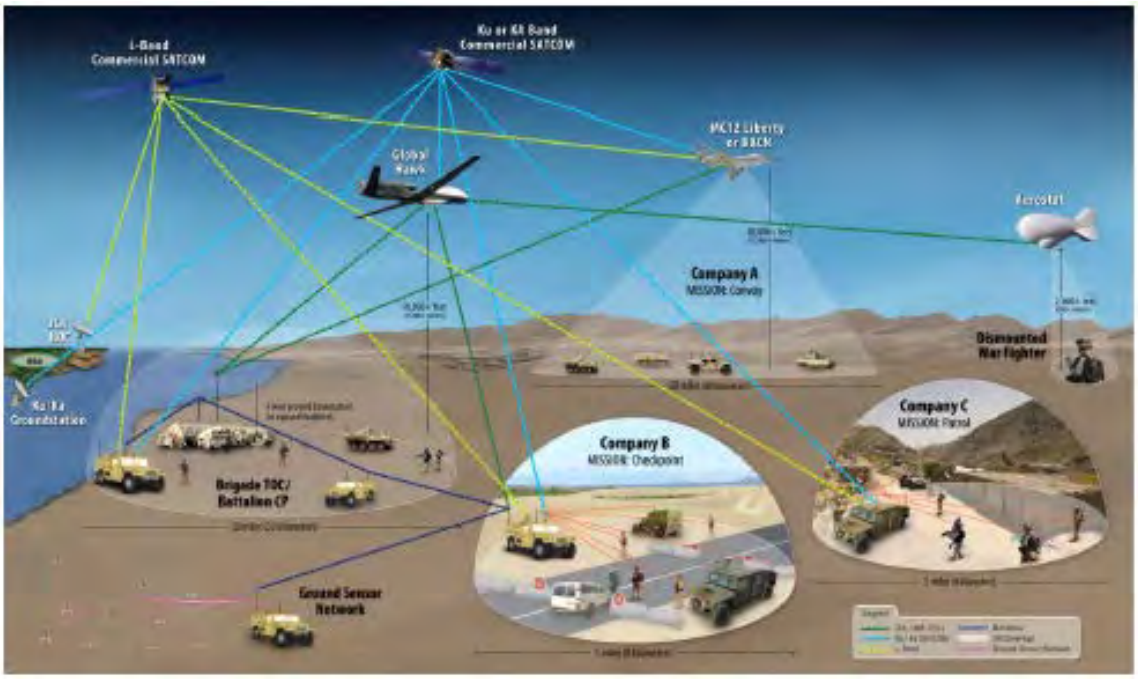

Figure 2. Oceus Networks Concept of Operations (from Liguori & Daniel, 2013)

Of the primary innovations from Oceus Networks is the Xiphos Base Station. The Xiphos Base Station, as shown in Figure 3, was in operation in 2013 with both the U.S. Army and the U.S. Navy, which was conducting pilot tests with the system. As a result of its employment, the Army has currently contracted to purchase 36 Xiphos Systems (Liguori & Daniel, 2013).

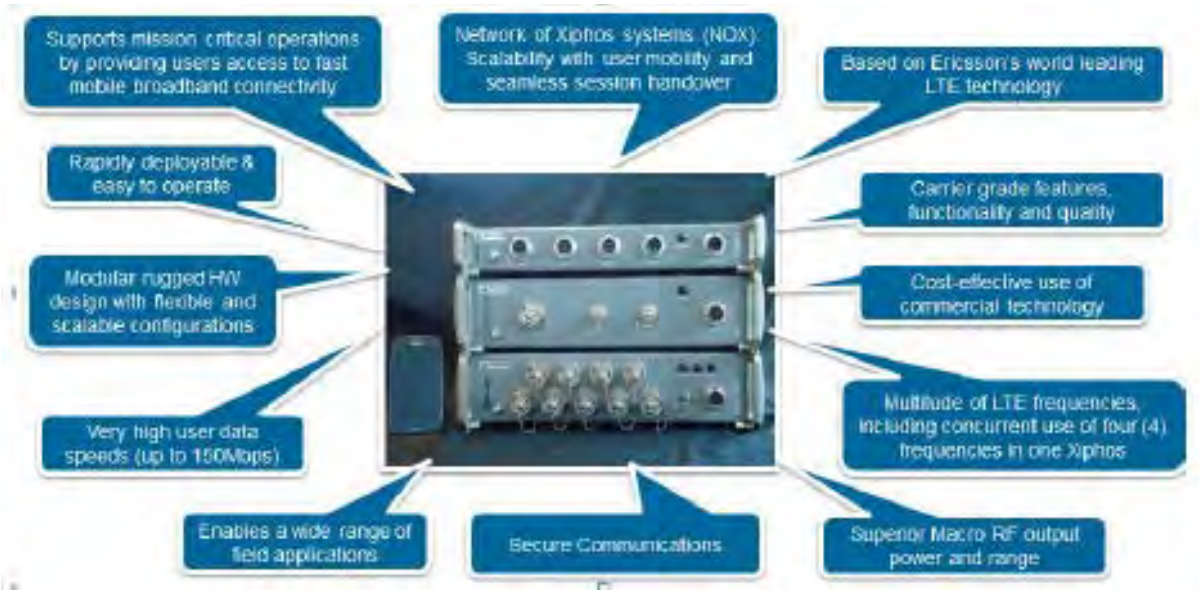

Figure 3. Xiphos Base Station (from Liguori & Daniel, 2013)

The Xiphos comes in two different configurations which are the "1 Radio Unit" (1 RU), which services from 100 to 200 tactical cellular connections, and the larger "6 RU" configuration, which can handle approximately 1200 connections (Liguori & Daniel, 2013). The 1 RU Xiphos is suited for a tactical USMC unit of approximately Company size, while the larger 6 RU Xiphos is more suited for a significant-sized Forward Operating Base (FOB) on the scale of Camp Leatherneck, Afghanistan. For example, a typical Infantry Battalion or Marine Expeditionary unit (MEU) would require five "1 RU" Xiphos Base Stations (Liguori & Daniel, 2013). Xiphos uses Ka band technology for backhaul, and can interface with either military satellites or commercial satellites, such as the O3b Networks COMSATCOM constellation. The Xiphos 4G/LTE system spans the three operational scenarios of fixed, dismounted, and OTM, thereby providing information to the tactical edge of the battlefield (Liguori & Daniel, 2013).

B. CURRENT DOD AND USMC AND POLICY

As Liguori and Daniel (2013) asserted, both the military and commercial sectors have explored the concept of a Secure Mobile Cellular (SMC) capability for use by expeditionary forces. Both of these evaluators seek to expand their capabilities and information sharing, while preserving the security of sensitive data. In the private and

commercial sector, however, cellular capabilities are tailored to meet market demands, which have not yet shown a high degree of interest for highly secure cellular services beyond specific small-scale purchases by the U.S. government. Because of this lack of demand, as well as the obvious accompanying risks associated with unsecure communications, the DOD lags behind commercial entities in terms of adopting mobile computing technologies.

Nevertheless, the DOD and USMC are taking steps to close the gap of highly mobile communication devices that have voice and data capabilities (Liguori & Daniel, 2013). These steps do not entail purely embracing the newest technology, but rather focus on keeping the DOD workforce relevant in an era when information, its accessibility, and the capability to process it play an increasingly critical role in mission success (Cox, 2013). Through the policy formulation process, which will be described later in this paper, the DOD assumes the lead in developing policy that guides Marine Corps strategy. Assessing the documents which stem from this simple top-down approach, the policies and strategies in Figure 4 demonstrate an evolution in thinking for operating in non-traditional workspaces from top to bottom guidance. The ability to raise situational awareness at all levels of deployed Marine Corps units may enhance mobility across the war fighting functions. As shown in Figure 4, the top-down DOD policies and strategies show a trend to leverage COTS technology in mobile computing (Liguori & Daniel, 2013).

Figure 4. DOD and USMC Policy and Strategy for Mobile Devices (from Liguori & Daniel, 2013)

1. DOD Mobile Device Strategy

Recognizing the current uses and future capabilities that mobile devices offer, the DOD Chief Information Officer (CIO), Teresa Takai, published the DOD Mobile Device Strategy in 2012 in order to capitalize on the full potential of mobile devices (Office of the Department of Defense Chief Information Officer, 2012). As defined by the DOD Mobile Device Strategy, a mobile device is a

> handheld computing device with a display screen that allows for user input. When connected to a network, it enables information sharing in formats specially designed to maximize the use of information given device limitations. (Office of the Department of Defense Chief Information Officer, 2012, p. i)

The increasing use of smartphones and tablet computers, which provide a continuous link to the Internet, social media, and apps has made information sharing not merely a capability, but an expectation, particularly among younger service members who have grown up with it at their fingertips. The DOD challenge becomes to support the users requiring access to information anywhere and anytime across the DOD Information Enterprise (IE), facilitating making informed decisions in the execution of the assigned mission (Office of the Department of Defense Chief Information Officer, 2012, p. 2).

The DOD CIO's implicit vision is to have a highly mobile workforce equipped with secure access to information and computing power anytime and anywhere (Office of the Department of Defense Chief Information Officer, 2012). Providing deployed personnel with a secure smartphone capability is directly linked to this vision (Liguori & Daniel, 2013). The DOD Mobile Device strategy also highlights the need for ubiquitous information sharing through mobile computing for units maneuvering in austere and unfamiliar environments. Applications and capabilities, from real time map data—to assessing medical lab results remotely, would certainly be of benefit to expeditionary military units (Office of the Department of Defense Chief Information Officer, 2012).

a. Strategic Goals

The DOD seeks to create a wireless infrastructure based on existing networks in order to provide accesses for wireless mobile devices to enable warfighters to profit from

mobile computational power. The wireless infrastructure is an expansion of the current DOD IE which can be leveraged to connect mobile capabilities and technologies. The DOD must focus on three critical areas central to mobility: the wireless infrastructure, the devices themselves, and the applications the devices use (Office of the Department of Defense Chief Information Officer, 2012). With these critical areas in mind, the DOD defined three major goals, depicted in Figure 5, each with practical implementation subcomponents which the DOD named objectives:

GOAL	DESCRIPTION
1. Advance and evolve the DoD Information Enterprise infrastructure to support mobile devices	Improves wireless infrastructure to support the secure access and sharing of information via voice, video, or data by mobile devices.
2. Institute mobile device policies and standards	Establishes policies, processes, and standards to support secure mobile device usage, device-to-device interoperability, and consistent device lifecycle management.
3. Promote the development and use of DoD mobile and web-enabled applications	Provides the processes and tools to enable consistent development, testing, and distribution of DoD-approved mobile applications for faster deployment to the user. Establishes policy, processes, and mechanisms for appropriately web-enabling critical DoD IT systems and functions for mobile devices.

Figure 5. Goals of the DOD Mobile Device Strategy (from Office of the Department of Defense Chief Information Officer, 2012)

Goal 1. *Advance and evolve the DOD Information Enterprise infrastructure to support mobile devices*. – The intent behind this goal is to improve the existing wireless backbone to support secure voice, data, and video capabilities for mobile devices. Moreover, the DOD also looks to reduce the tethering of individuals to desks, as well as potentially to reduce costs for office space and desktops and other hardware (Office of the Department of Defense Chief Information Officer, 2012).

Objective a. *Evolve spectrum management*. The DOD understands the need to manage what is a finite electromagnetic spectrum as the explosion of wireless networks puts added stress on an already constrained allocation system. Particularly, the DOD turns its attention to academia to expand and improve up on current multiple access techniques (Office of the Department of Defense Chief Information Officer, 2012).

Objective b. *Expand infrastructure to support wireless capabilities*. With the ideal being a wireless unclassified and classified mobile network, the DOD desires to base its infrastructure off of the industry standards of the IEEE 802.11-based Wide Local Area Network (WLAN) as well as commercial 4G technology (Office of the Department of Defense Chief Information Officer, 2012).

Objective c. *Establish a mobile device security architecture*. Perhaps one of the most challenging elements of the mobile device strategy, the need for a secure mobile architecture is underscored by the myriad traditional and novel security risks. Specifically, the DOD plans to mitigate some of these risks through the inclusion of PKI security, access, and identification controls at all levels of the architecture, to include the application, device, and network (Office of the Department of Defense Chief Information Officer, 2012).

Goal 2. *Institute mobile device policies and standards*. – The intent behind this goal is to create a top-down framework to govern device usage, interoperability, and device lifecycle management (Office of the Department of Defense Chief Information Officer, 2012).

Objective a. *Develop mobile device policy and standards*. As mentioned earlier, while the cost-savings potential to use commercial off the shelf (COTS) devices is tantalizing, most do not come fully equipped to meet the DOD security needs. Hence, the DOD desires to expedite and standardize technology development in a fashion which offers the ability to rapidly incorporate new commercial advances, while also allows DOD modification and security enhancement. Additionally, the DOD plans to evaluate the use of personally owned devices critically in order to gain efficiencies while maintaining network security (Office of the Department of Defense Chief Information Officer, 2012).

Objective b. *Establish a mobile device management service*. This service would attempt to manage mobile devices centrally to the extent that they need licensing, registration, and continuing software and security upgrades as well as to monitor network usage and health (Office of the Department of Defense Chief Information Officer, 2012).

Objective c. *Educate and train mobile device users*. Another equally essential element in this strategy is the increased levels of trust required between network administrators and the individual user, particularly where a bring your own device (BYOD) architecture is concerned. The DOD's recognition that in many cases, user-based enforcement of security measures is the only effective approach, and that such a measure will require additional training for the force to underscore its importance (Office of the Department of Defense Chief Information Officer, 2012).

Goal 3. *Promote the development and use of DOD mobile and web-enabled applications*. – The intent behind this goal is to outline processes and standards for application development, testing, and fielding within the DOD to ensure more rapid distribution of approved DOD mobile applications to the end users, as well as a web-based support service for mobile devices and applications (Office of the Department of Defense Chief Information Officer, 2012).

Objective a. *Establish a common mobile application development framework*. Whereas commercial entities frequently provide pre-made kits to assist with development and testing of new applications, these kits are operating system specific, and therefore pose limited utility in a more heterogeneous DOD environment. With a primary focus on interoperability, the DOD intends to leverage commercial capabilities, and indeed may go so far as to instruct components how to use commercial app building kits, while also adding in guidelines to support OS-generic operation. Perhaps the most challenging aspect of this framework would be the requirement to evolve as industry standards advance, as the DOD is not known for rapid policy evolution (Office of the Department of Defense Chief Information Officer, 2012).

Objective b. *Institute a mobile application certification process*. In anticipation of the profusion of new applications, the DOD perceives the need for a centralized and standardized application certification process which is both more comprehensive and swifter than its current model. Most specifically, the DOD is concerned with ensuring applications are free from known exploitable vulnerabilities, are interoperable, and can be monitored to enforce compliance with policy and regulation (Office of the Department of Defense Chief Information Officer, 2012).

Objective c. *Provide an enterprise mobile application environment*. Going hand in hand with the previously described certification process, the DOD also sees the need to provide a total mobile application environment to support the creation, certification, fielding, and maintenance of mobile applications across the DOD. The DOD seeks to federate application creation in an effort to reduce costs by making approved apps and derivatives more widely available for reuse as well as incorporating tracking features into apps such that upgrades and other system lifecycle events are easily executed. The DOD focus for this objective is on the app submission, development, certification and approval, management, and compliance processes (Office of the Department of Defense Chief Information Officer, 2012).

Objective d. *'Web-enable' IT capabilities for mobile device support*. Concerned with the growing pace of technological advancement, the DOD grasps the need to develop a web-enabled IT support system for mobile devices and applications. This support would cover elements from display and presentation upgrades, to software and security features (Office of the Department of Defense Chief Information Officer, 2012).

2. Guidance from Senior USMC Leadership

In a combination of current DOD policies and the war time experiences of the past decade, it becomes clear that the USMC seeks to return to its roots as America's expeditionary force in readiness. A strong focus on command and control (C2) will aid in the evolution to a mobile force (Liguori & Daniel, 2013). As stated in MCDP-6,

> No single activity in war is more important than command and control. Command and control by itself will not drive home a single attack against an enemy force. It will not destroy a single enemy target. It will not affect a single emergency resupply. Yet none of these essential war fighting activities, or any others, would be possible without effective command and control. Without command and control, campaigns, battles, and organized engagements are impossible, military units degenerate into mobs, and the subordination of military force to policy is replaced by random violence. In short, command and control is essential to all military operations and activities. (U.S. Marine Corps, 1996, p. 35)

The communication processes which unify the other war fighting functions (Maneuver, Fires, Intelligence, Logistics and Force Protection) fall under the theme of

C2. In the current fiscally constrained environment, and having an appreciation for the requirement to be more mobile than ever before, the senior leadership guidance for the way ahead focuses on leveraging military and COTS technological innovation to enable increasingly decentralized command, rapid feedback, and improved decision making at all levels of the force (Liguori & Daniel, 2013).

3. Priorities of the 35th USMC Commandant

The 35th Marine Corps Commandant released his 2010 planning guidance in order to outline his priorities and set the tone for the Marine Corps. He noted that, "The future will be different from the world we knew prior to the attack on 9-11. Through innovation and willingness to adapt, we will remain the ready and relevant force America relies on in times of crisis" (U.S. Marine Corps, 2010a, p. ii). Of particular note in this guidance is the discussion of rebalancing the Marine Corps for the future by aggressive experimentation and the intent to implement new capabilities. Also as shown in Figure 6, the Commandant emphasized that the focus must be on training Marines for distributed operations and increasingly complex environments. These strategic planning factors shape the need for a highly network-enabled device to provide the tactical Marine with enhanced situational awareness and to increase information sharing across the war fighting functions.

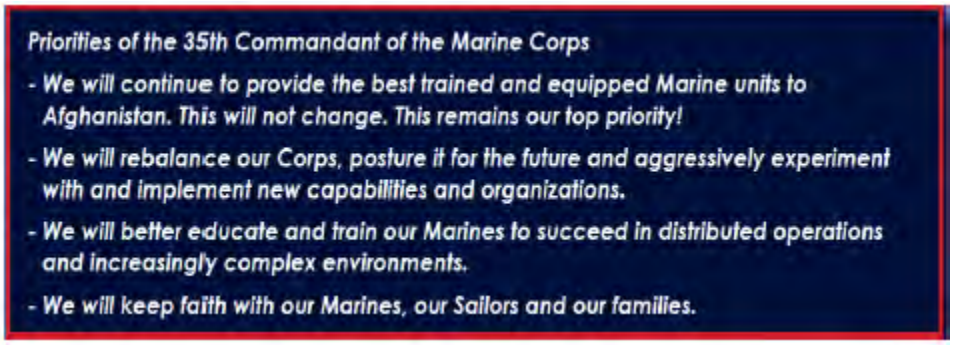

Figure 6. 35th USMC Commandant Priorities (from U.S. Marine Corps, 2010a, p. 8)

4. USMC Vision and Strategy 2025

In 2010, the Commandant also published the Marine Corps Vision and Strategy 2025 which aims to posture the USMC for the future through an elucidation of a common outlook. Within the strategy, the Commandant detailed ten task clusters grouped into three main themes:

- Focus on the Individual Marine: Improve Training and Education for fog, friction and Uncertainty – Posture for hybrid threats in complex environments – Build and deploy multi-capable MAGTFs (U.S. Marine Corps, 2010b).
- Expand persistent forward presence and engagement – Lead Joint Operations and enable interagency activities (U.S. Marine Corps, 2010b)
- Reinforce naval relationships – joint sea basing capabilities—Focus on amphibious force levels (U.S. Marine Corps, 2010b)

As might be discerned, the first theme assumes the information sharing and processing capacity implied in the mobile device strategy and senior Marine Corps Leadership guidance. As such, this theme prompted the development of command and control systems for improving the situational awareness of the individual Marine. To keep the Marine Corps systems development objectives aligned to the strategy, Marine Corps Systems Command (MARCORSYSCOM), Quantico Virginia issued the following guidance internally in 2012 via the program manager of MAGTF Command, Control and Communications:

- Develop necessary capability and capacity to effectively operate in the information environment (Reddy, 2012).
- Integrate command and control (C2) and Individual Squad Radios (ISR) capabilities down to the squad level (Reddy, 2012).

5. USMC MAGTF 2012 C2 Roadmap

The Marine Corps released its 2012 roadmap for MAGTF C2 in 2012. This strategy document focuses on providing the right information to the right Marine at the right time in order to make timely and informed decisions (Marine Corps Combat Development Command, 2013). The core tenants of the roadmap orient the Marine Corps to develop C2 systems given the current and future information environment and seek to

aid in defining overarching capability. The core tenants as stated in the 2012 MAGTF Roadmap are:

- Commander and Leader centric
- Network enabled
- Information assurance
- Collaborative, shared situational understanding
- Performed at all echelons
- Performed anywhere in the battlespace

These six tenants guide the conceptualization and development of systems away from a system-centric approach and to more of a user focus that enhances leader-centric, network enabled operations (Marine Corps Combat Development Command, 2013). The C2 roadmap outlines the basic elements of C2 as people, information, procedures, as well as a support structure for the people who create, disseminate and use information (Marine Corps Combat Development Command, 2013). To enable information and raised awareness at all levels, the concept of being "Network enabled" is a critical evolutionary component in preparing Marine Corps forces for the future. "The current network infrastructure must transition to a tightly integrated, agile, defensible, survivable network capable of supporting widely distributed operations" (Liguori & Daniel, 2013).

6. USMC Commercial Mobility Strategy 2013

In 2013, the USMC Director for Command, Control, Communications, and Computers (C4) released the USMC Commercial Mobility Strategy to further guide and execute the above policies and guidance. Specially, through the Commercial Mobility Strategy, the Marine Corps sought to align DOD and Marine Corps Strategies in conjunction with the current DOD priority to consolidate data centers in an effort to enable a cloud computing environment (Command, Control, Communications, and Computers [C4], 2013). General Kevin Nally, Director C4, stated, "With increasing mobile device capabilities, the Marine Corps recognizes the trend of evolving information needs within garrison and tactical environments and the need to provide an agile method of meeting those needs" (C4, 2013, p. 3). The USMC Commercial Mobility Strategy focuses on the device user and the ability to share information via platform

agnostic programs and applications. The underlying driver behind this focus is that raised situational awareness stemming from information sharing, both in garrison and deployed roles, will enable more efficient mission accomplishment (Liguori & Daniel, 2013). Furthermore, as General Nally contended, as the user gains flexible and ubiquitous ability to share information effectively to raise situational awareness and reduce decision-making timelines, the increased capacity to access, share, and manipulate data and information will provide users enhanced freedom of movement across the seven war fighting functions (C4, 2013). As stated in the USMC Commercial Mobility Strategy (2013) the four goals are:

- Establish a Secure Mobile Framework
- Transition the Unclassified Mobile Device Infrastructure to a Cost Effective and Platform Agnostic Environment
- Collaborate with DOD and Industry Partners to Develop a Classified Mobile Device Capability
- Incorporate Personally Owned Mobile Devices

C. DOD AND USMC SECURITY POLICY

1. DODI 8500.01: Cybersecurity

Published in March 2014, the new DODI 8500.01 cancelled the legacy Information Assurance Instruction (8500.01E, April 2007) as well as ten other DODI and memoranda (Department of Defense, 2014b). Critical aspects of this instruction outline that cybersecurity will be integrated into all aspects of system lifecycles, with the subsequent corollary that cybersecurity personnel must therefore also be fully integrated into all phases of system development lifecycles.

DODI 8500.01 goes on to discuss that the DOD will make public key (PK) encryption the standard for all DOD information systems and will "implement a DOD-wide PKI solution that will be managed by the DOD PKI Program Management Office" (Department of Defense, 2014b). Furthermore, DODI 8500.01 provides for the inclusion and incorporation of biometrics to assist in support of identity assurance. DODI 8500.01 also mentions the desirability for systems to be able to self-reconfigure and self-recover against attacks wherever possible.

In addition to the requirement to develop and maintain sufficient cybersecurity protocols for all DOD information systems, and to protect DOD information with requisite levels of confidentiality, integrity, and availability, DODI 8500.01 also lays out responsibilities and procedures for this policy throughout the DOD. A discussion of the cybersecurity procedures will follow.

a. Enclosure 3 (Procedures) to DODI 8500.01

Enclosure three to DODI 8500.01 focuses on a plethora of cybersecurity topics ranging from operational resiliency to requirements of the cybersecurity workforce. However, the first subject area addressed is that of risk management, and as such this paper will mention that area first as well.

DODI 8500.01 identifies that cybersecurity risk management is a subset of acquisition risk management. Logically then, the risk assessment process for cybersecurity would extend to the logistical support apparatus required to maintain the integrity of the fielded equipment (Department of Defense, 2014b). In other words, much as initial operational spares and replacement and upgrade considerations must be part of the deliberate planning and risk assessment for any project, cybersecurity upgrades, refreshes and maintainability items must be included in risk management discussions. To that end, the DOD CIO identified a three-tiered approach to cybersecurity risk management as outlined in Figure 7 below, as well as a separate risk management framework (RMF), which is described in DODI 8510.01.

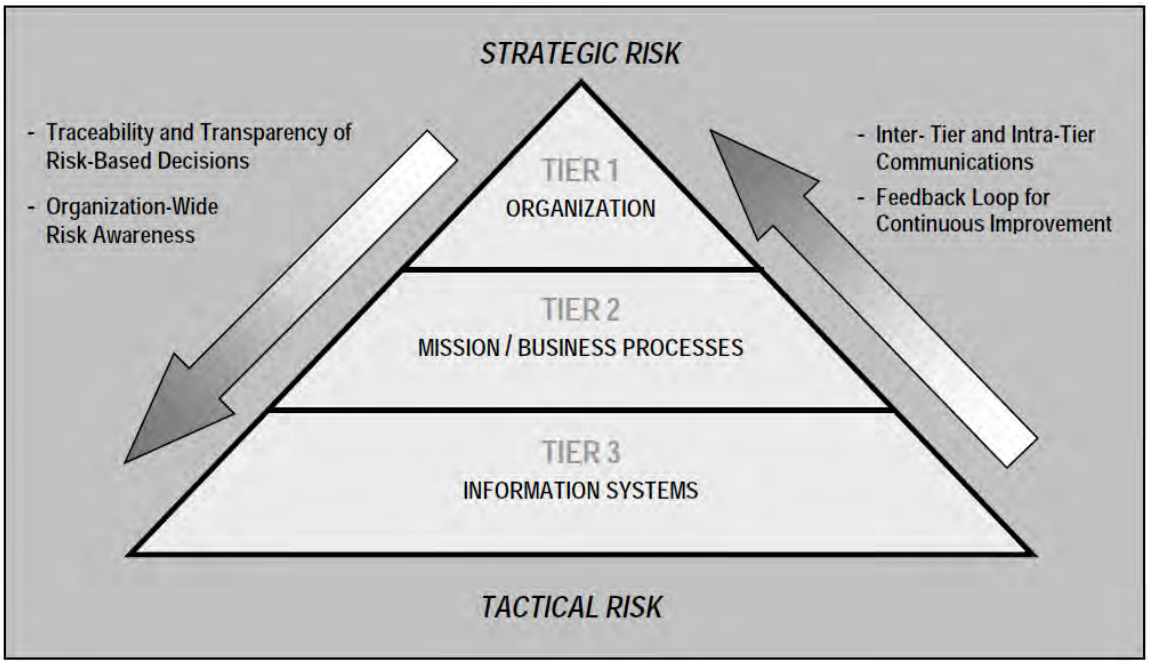

Figure 7. Three-Tiered Approach to Risk Management (from Department of Defense, 2014b, p. 28)

The key items to note from this diagram are that risk management decisions flow both ways in the organization in that while the tactical decisions are guided by the organizational perspective from tier 1, tiers 1 and 2 are also influenced by the decisions made at tier 3.

Other items of note from enclosure three are the decision to protect all DOD IS in accordance with National Security System security controls, the requirement to plan and resource penetration and exploitation testing during the developmental test and evaluation (DT&E) and the operational test and evaluation (OT&E) phases of the acquisition cycle, and finally the emphasis on a net-centric approach to cybersecurity. In the net-centric approach, DODI 8500.01 encourages the use of modern interconnectedness to "form new capabilities and teams without being constrained by geographical, organizational, or technical barriers" (Department of Defense, 2014b, p. 32). In addition, enclosure three obliges DOD IS' to provide for compatibility and authentication processes for use by coalition mission partners, to include a PKI application designed for foreign nationals.

The overarching theme running through DODI 8500.01 is that of holistic security. While each subsystem and indeed each piece of DOD information should enjoy a level of security commensurate with its status, the central idea is that no IS or piece of information should degrade the systems or enterprise to which it is interconnected (Department of Defense, 2014b). In effect, due to such interconnectedness, any one link in the cable may prove to be the weakness by which an adversary gains an advantage, and so testing and security considerations cannot view a system as a stand-alone entity, and instead must also account for ways in which one system's weaknesses may expose those that link to it to risk.

2. DODD 8000.01: Management of the DOD Information Enterprise

In standard hierarchical fashion, management of the DOD IE flows downward from the Secretary of Defense to the heads of the DOD components, and then to chief information officers (CIO) at each of the DOD components. DODD 8000.01 formally outlines the responsibilities of the heads of the DOD components as well as the Chairman of the Joint Chiefs of Staff to appoint CIOs over their respective components as well as a joint community CIO (Department of Defense, 2009b). It then becomes the responsibility of these CIOs to head an office which ensures their entity complies with DOD policies, to participate in forums concerning the governance of the DOD IE, and to train and retain IT personnel pursuant to the aforementioned responsibilities (Department of Defense, 2009b).

DODD 8000.01 calls for a review of all IT investments to ensure continued compliance with the DOD enterprise architecture, IT standards, and other related policy requirements (Department of Defense, 2009b). Finally, and critically, from a high-level viewpoint, DODD 8000.01 encourages the use of pilot programs, modeling and simulation, experimentation, and prototyping to reduce the risk of large high-risk projects. Of note, however, is that such experimentation is not to be used in lieu of the formal acquisition processes when implementing a production version of the solution (Department of Defense, 2009b).

3. DODI 8320.02: Sharing Data, Information, and Information Technology Services in the Department of Defense

DODI 8320.02 seeks to establish policies, processes and responsibilities to ensure the secure sharing of electronic data, information, and IT services within the DOD (Department of Defense, 2013b). While the instruction applies to all data assets, information, and IT services within the DOD enterprise, in development, and in the larger community of interest (COI), it specifically does not apply to currently deployed systems for which modernization investment dollars have not been received (Department of Defense, 2013b).

DODI 8320.02 requires that all DOD activities meet approved and applicable standards and specifications as found in the DOD IT Standards Registry (DISR), and tasks component heads and CIOs to ensure assets are in compliance with these standards or have an appropriate waiver in accordance with DODD 4630.05. DODI also instructs that DOD IT assets protect data both in transit and at rest commensurate with the assets' confidentiality level, mission assurance category, and level of exposure (Department of Defense, 2013b).

4. DODI 8510.01: Risk Management Framework for DOD IT

DODI 8510.01 replaced the previous DOD Information Assurance Certification and Accreditation Process and manages the cybersecurity risk for DOD IT from a total life-cycle perspective (Department of Defense, 2014c). The policy goals behind DODI 8510.01 are the establishment of an enterprise-wide RMF decision structure for cybersecurity in order to ensure consistency of the DOD IE with the National Institute of Standards and Technology Special Publication 800-37.

As an aspect of the RMF process, a plan of action and milestones (POA&M) must be developed and maintained to addresses all known vulnerabilities of IT systems, and continuous monitoring will be used wherever possible (Department of Defense, 2014c). The RMF process is to inform the DOD acquisition processes for all DOD IT, to include both DT&T and OT&E, but does not formally replace these processes.

Lastly, DODI 8510.01 encourages reciprocal acceptance of DOD and other federal agency and department IT system authorizations, with refusals reported to the DOD component senior information security officer. The instruction notes that reciprocity "is an essential element in ensuring IT capabilities are developed and fielded rapidly and efficiently across the DOD Information Enterprise" (Department of Defense, 2014c, p. 21). Furthermore, reciprocity reduces the need for redundant testing.

The development of an RMF for an IS and platform IT (PIT) closely follows the system development life cycle as shown in Figure 8.

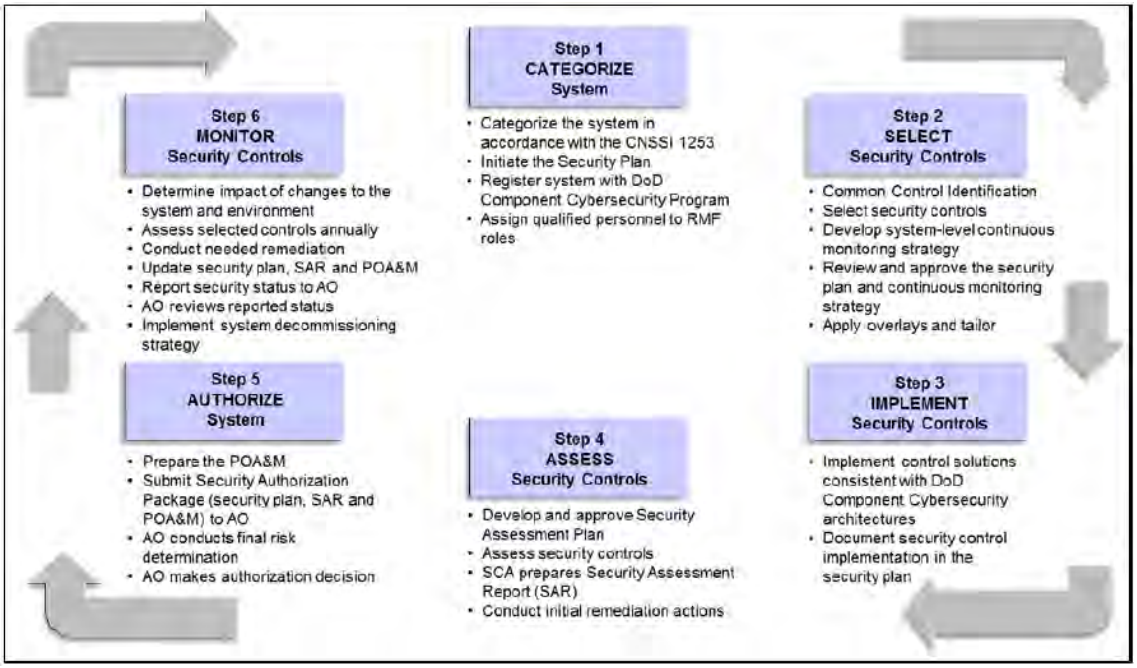

Figure 8. Risk Management Framework for IS and PIT (from Department of Defense, 2014c, p. 28)

Through application of the methodical security implementation process outlined in DODI 8510.01, development of adequate security controls for IS and PIT appears a near certainty.

5. DODI 8520.02: PKI and PK Enabling

DODI 8520.02 prescribes the procedures and authorities necessary to establish and implement and DOD-wide PKI in order to enhance DOD IS through PKI-enabled

authentication, digital signatures, and encryption (Department of Defense, 2011). Put simply, it is DOD policy that for all systems on the Non-classified Internet Protocol Router Network (NIPRNET) and the Secure Internet Protocol Router Network (SIPRNET) the DOD shall enable PKI use for digital signatures and encryption as well as for authentication. Where applicable, the PKI will be implemented via the CAC in accordance with Federal Information Processing Standards Publication (FIPS) 201-1, Personal Identity Verification of Federal Employees and Contractors) (Department of Defense, 2011).

DODI 8520.02 provides authority to the CIO to approve DOD hardware tokens other than the CAC for identity, authentication and signature. It also instructs heads of the OSD and the DOD components to plan, program, budget, and test to support the evolution and continued efficacy of PKI within the DOD IE, and charges them to implement PKI on IS in the areas of network login, email, web servers, and devices. These requirements pertain equally to COTS and government-developed systems (Department of Defense, 2011)

Furthermore, DODI 8520.02 specifies that the CAC will be the primary hardware token used for access to NIPRNET systems, and hardware tokens for the SIPRNET shall be used in accordance with national security systems (NSS) PKI (Department of Defense, 2011). Alternate tokens can be authorized on a case by case basis in circumstances where authentication certificates on the CAC cannot be used by various groups of users, and are approved via a service or agency-level certificate practice statement (CPS) (Department of Defense, 2011).

D. DOD POLICY FORMULATION PROCESS

Being a subset of the DOD, the USMC makes policy in accordance with the guidance, directives, and policies from the DOD, which often publishes strict security policy guidance regarding networks and communications. As the USMC proponent for communications and networks, HQMC C4 sits on multiple working groups at the DOD CIO and DON CIO levels pertaining to mobility. In addition to the C4 representative, numerous other stakeholders are usually present to include all of the other armed

services, DISA, and the NSA, totaling 10–20 persons present with others joining via teleconference. For policy to become effective, the products of these working groups comes out as a Joint Task produced by action officers, and then sent up the chain of command from O-6 levels to Flag and General Officer levels. At this point the service level organizations, such as C4, review the policy and submit feedback, suggested revisions, and comments. After collating the returns from the various stakeholders, the DOD CIO office publishes new policy. As the policy comes from the DOD CIO, the USMC does not always publish its own independent version, though C4 can if it so chooses (R. Anderson, interview with the author, April 29, 2013).

DISA manages a listing of approved devices which all DOD entities may use in certain capacities which it review semi-annually or on demand if a new device is available which a unit wants to use. This is the Unified Capabilities Approved Products List (UCAPL). If a device is in line with the current UCAPL and existing security policy, a fairly rapid review process takes place which allows it to be implemented.

When a new device or capability is available which the USMC desires to use but which does not fall within the current UCAPL and security policy, the USMC must first provide this input to its working groups. In order for the product to be considered, the USMC must show that the technology is feasible and then request a waiver for a pilot program. For the USMC, the waiver process starts as a conversation at the General Officer level between the Director C4, and the DOD CIO. The DOD CIO will then push the waiver request to the Mobility Project Manager, and then the request will be pushed from action officer to action officer before approval. This process can take months.

Once the request is approved, the USMC can then begin testing its pilot program. Following success in the pilot, the USMC then requests and is ultimately granted a permanent waiver to allow it to operate its program until new policy is published. Concurrently, the DOD must then rescind its earlier policy, begin the policy formulation mark-up process between all of the stake holders, and then republish its policy. There is no specific set of criteria for how this process happens. Instead, it is known informally as the way staff work is done at the Pentagon and within the larger DOD (R. Anderson,

interview with the author, April 29, 2013). This process will be broken down step by step in later chapters for further analysis.

III. CASE OF FIST/LIGHTHOUSE

As the primary example to elucidate current USMC uses of smartphone technology, this paper will portray the use of hand-held collection platforms through the case study of the Lighthouse/FIST projects at NPS. This example is ideal in that it encompasses the duality of the core of this thesis: a cutting-edge system which presents real potential benefits, real risks, and which is in the throes of the policy approval process. To clarify the distinction between the two systems, both FIST and Lighthouse were born of Longley's 2010 NPS thesis. While the Common Operational Research Environment (CORE) Lab at NPS retained cognizance and control over the Lighthouse version, keeping it in tighter line with DOD requirements and a central mission of social network analysis, the FIST project broke away and while also associated with NPS, is sponsored by the Counter-Narcoterrorism Technology Program Office, and hosted by the Kestrel Corporation (Office of the DOD CIO, 2013).

A. FIST OVERVIEW

As Longley (2010) attested, the decision to adopt Commercial Off-the-Shelf (COTS) technology and use a rapid prototyping process has enabled the FIST team to move from a concept to a product in the field more quickly than would have been possible through the traditional DOD procurement process. The time saved by using COTS greatly reduced the currently arduous military procurement process, which lags far behind rapidly advancing technology (Longley, 2010).

FIST is a field data-collection system which incorporates COTS smartphones, a customized software package, and a robust information management support system called *FusionPortal* with a deployable sensor fusion system known as *FusionView* (Longley, 2010). As Longley (2010, p. 1) asserted, "*FusionView* enables real-time integration of disparate sensor systems that provides a powerful common operating picture critical for today's decision makers." Furthermore, using *FusionPortal*, data can be exported and analyzed using geospatial, geo-statistical, temporal, link, and social network analysis. Use of the portal also facilitates the exchange of information with

external databases such as the Worldwide Civil Information Database (WCID), the International Studies of Violent Groups (ISVG), and the Combined Information Data Network Exchange (CIDNE) (Longley, 2010).

Longley (2010) also described how "FIST facilitates ease of information collection through a user-friendly interface, and enables information to flow from the point of capture to analysts in near real-time regardless of location or physical proximity." FIST is well suited for operations across a variety of environments, ranging from temperate to austere, and to support a plethora of mission sets such as counterinsurgency operations (COIN), counter-narcotic missions (CN), and humanitarian assistance and disaster response (HA/DR). "The predominant principle of FIST is the development of a user-friendly data collection tool (Collect) that utilizes automated information systems to enable unstructured data to be collected, processed, and structured for analysis and visualization in a variety of analytic packages" (Longley, 2010, p. 1).

Through the use of this system, the USMC seeks to capitalize on all of the advantages of smartphones in the commercial and private sector and apply them to military information collection. From the Marine Corps' standpoint, its current philosophy of "Every Marine a Collector" blends well with FIST's objective, which is a recognition of the need to equip as many people as possible in the operating environment to fully realize the potentials of a robust data-collection system (Longley, 2010). As Longley (2010) described, too often a collection capability is entrusted to the hands of a limited few, which restricts the scope and utility of data collection. Therefore, by designing FIST to operate on smartphones, harness the power of Web technologies, and present information on a lightweight visualization system, data collection, analysis, dissemination, and utilization can occur on a much broader scale than with previous systems (Longley, 2010).

a. Use Potential in HA/DR Missions

Humanitarian Assistance and Disaster Relief (HA/DR) missions impose significant challenges with regards to information technology and communication. Relief agencies need massive amounts of information, which hinges on connectivity, to assess

the areas most affected, to tailor specific packages to local needs, and to gauge measures of performance and effectiveness. Unfortunately for those seeking to ameliorate the situation, all too frequently the local infrastructure is destroyed (DR) or non-existent (HA), and the information they so desperately need is lacking due to a dearth of connectivity. FIST offers an interim solution to this shortfall in that not only can the relief actors collect and view information through the portal, but smartphones could also be handed out to locals on the ground so that they might self-populate the portal. Needless to say a short anecdote should serve to illustrate the point.

In the wake of the earthquake that devastated the impoverished country of Haiti in 2010, the Kenyan-based company Ushahidi jump-started what became an international crowd-sourced relief effort which relied on texts coming from the people on the ground. Ushahidi was then able, after some substantial coordination efforts, to geotag and link the texts with footage from U.S. Army unmanned aerial vehicles (UAV) (Tapscott & Williams, 2012, p. 4). The end result was a near-real time geographical depiction of user-generated reports and needs to which any relief worker could subscribe via the public internet. Better yet, the entire enterprise was accessible via smartphone (Tapscott & Williams, 2012, pp. 4–7). This meant that although each relief organization likely had stove-piped information systems and hierarchical chains of command, all could access the list of needs and see visually where the resources were required without any need for formal information sharing or coordination. From this small example, it becomes quite clear the use potentials for smartphone enabled technologies in HA/DR situations.

b. Use Potential in COIN Missions

As with the HA/DR situation described above, the potential uses of a FIST-like system in a COIN environment are myriad and obvious. Collection of biographic and cultural data on areas, structures, capabilities, organizations, people, and events (ASCOPE) and political, military, economic, social, information, infrastructure factors (PMESII) is tine-intensive and requires patrols physically going to the locales, which puts troops at risk. After all the effort to collect the data, it might be entered into any number of databases (MarineLink, CIDNE, TIGR, Palantir, CPOF, etc.), and in any type of

format. Worse yet is if the data, once collected, goes nowhere other than into a small notebook which is discarded at the end of the deployment. FIST changes this mindset. By making data entry easier and more accessible than Biometric Automated Toolset (BAT), Handheld Interagency Identity Detection Equipment (HIIDE), or Secure Electronic Enrollment Kit (SEEK) (current biometric and cultural data systems), and in concert with its lightweight and mobile nature, FIST justifies the risk to which troops are subjected during the collection phase and enable the population control which is so critical in a COIN environment. Naturally, application for use in a COIN environment implies the need to incorporate classified technology to the application which introduces an additional subset of security concerns above and beyond those mentioned as part of general smartphone vulnerability.

B. ISSUES ARISING FROM FIST'S INTRODUCTION, IMPLEMENTATION, AND USE

Three years after Captain Longley's initial idea to create a system to collect, process, and structure socio-cultural data in a streamlined fashion which would reduce time wasted by analysts in formatting data for analysis, and two years after he began work on the system as part of his thesis, Captain Longley demonstrated a working prototype during CARAT Thailand 10 in May 2010 (Roberts & Longley, 2013, p. 183). Along the way, Captain Longley was forced to change the name of the program from the human Terrain Analysis and Collection System (HTACS) to something more "vanilla;" Multi-modal Information Support Tool (MIST), a name which was already in use by other programs, and then finally to FIST (Roberts & Longley, 2013, pp. 179–182). Following a break with his former thesis co-advisor over private versus government ownership of the program, and the desire to use COTS and open-source technology, Captain Longley changed the name of the system from FIST to OpenFist, while the Kestrel Technology Group maintained control over the use of the name FIST and its proprietary software. Following threats of legal action from Kestrel Technology Group, which had filed trademark rights to FIST, and the potential for an unending brand-name battle between the NPS lawyers, administrators, multiple military commands, and contractors, Longley again changed the name of the system to Lighthouse (Roberts &

Longley, 2013, p. 188). From this contentious birth, two parallel systems (perhaps the divided assets of two divorced parents) emerged: FIST and Lighthouse. At the point of their split, however, a desirable, working prototype had already been demonstrated at the Sattahip Naval Base in Thailand in May 2010 and in Singapore in August 2010 (Roberts & Longley, 2013, pp. 183–184). This case study will pick up from that point and examine the divergent paths each system took in their quests for adoption into the DOD.

Despite the introduction of the critical components of FIST in 2010, and especially in light of the previously discussed USMC strategy and policy documents which highlight the intent to move toward increased use of smartphones, the program remains stymied, and full implementation into and use by USMC ground forces is severely limited. In an article from August 2012, Scarborough (2012a) documented the request for the Lighthouse from U.S. Special Operations Command (USSOCOM). Interestingly, Scarborough annotated that while USSOCOM intended to purchase Lighthouse because of its ability to "collect data via mobile devices…the internet and radios" USSOCOM then planned to upload that data into the Palantir system. At the conceptual level, this desire to link Lighthouse with Palantir for data analysis purposes appears counterintuitive since doing so would place FIST's data and analysis capacity into the proprietary hands of Palantir. Not surprisingly, the association of Lighthouse with Palantir brought the system into the on-going battle between Palantir and the Army's intelligence data network and analysis tool, the Distributed common Ground System (DCGS) (Scarborough, 2012a).

While the linkage between Palantir and Lighthouse caused immediate issues between supporters of the program of record DCGS and those of the COTS Palantir system, an attempt to decouple Lighthouse as a way to propel it forward also failed. Due to Lighthouse's ability to connect, interface, draw from and populate data into all manner of systems, in a meeting with DCGS program managers, representatives from the CORE Lab expressed interest in DCGS' analytical systems to assist with the social network analysis research it conducts (Scarborough, 2012b). Scarborough (2012b) also contended that one of the principal aims of the DCGS program managers in meeting with the CORE Lab was to convince them to integrate DCGS with Lighthouse. Furthermore,

Scarborough highlighted that the DCGS implied they would provide DCGS platforms free of charge to NPS to enable the integration. However, the lack of inclusion of COTS software into DCGS has resulted in Lighthouse remaining in fundamentally a research status at NPS, rather than a full-fledged system to support the warfighter; this despite the clear request for its capability from USSOCOM. Hence, Lighthouse did not get stone-walled by DOD or USMC policy per se, but rather by the internal politics and rivalries associated with program management in a resource constrained acquisition environment. While the zero-sum thought process of "any funding you receive is funding I lose," is antithetical to the open nature of Lighthouse's architecture, since it relies on COTS, that fact does not change the difficulties Lighthouse experienced in trying to integrate with existing systems. It is of singular importance that Lighthouse as it exists today was barely able to survive the competing pressure from for-profit contractors which stood to lose a lot of money if the program remained solely government owned and operated. That it endured at all in any form is a testament more to the hard work and dedication of the entrepreneur than to any policies which encourage bottom-up innovation within the DOD (Roberts & Longley, 2013, pp. 186–188).

Taking the more independent route, FIST attempted to market itself as a stand-alone system with its own organic back-end analysis capability. In this regard, FIST ran into DOD policy more directly, and more tellingly. In a memorandum from November 2013, the DOD CIO highlighted FIST as a commercially hosted capability operating contrary to DOD policy. Specifically, the memorandum cited FIST as "operating an unauthorized node on commercial network infrastructure that intersects with the DOD Non-classified Internet Protocol Router Network" (Office of the DOD CIO, 2013). Similar to the problems Lighthouse experienced with DCGS, in that there was little room for COTS to operate on a government-sponsored platform, FIST also ran afoul of DOD policy prohibiting the intersection of a commercial with a government network. Also like Lighthouse, in the period where USSOCOM coupled Lighthouse with Palantir and experienced a backlash from program managers of DCGS, the CIO memorandum charged FIST with duplicating the information sharing capabilities which already resided in a designated enterprise solution, the All Partners Access Network (APAN) (Office of

the DOD CIO, 2013). Specifically, FIST was found to be outside of compliance with regard to DODD 8100.04 DOD Unified Capabilities which outlines the requirements and process to obtain authority to operate on a DOD network (Office of the DOD CIO, 2013). DODD 8100.04 dictates the use of DOD enterprise services, and affords exceptions only when mission requirements and the best interests of the DOD necessitate them. In accordance with DODD 8100.04, the FIST program was instructed to provide documentation with its authority to operate, a review by the Defense Information Assurance Security Working Group and the Defense Information Systems Network Flag Panel, and its GIG waiver request within 14 days or be subject to censorship and punitive action (Office of the DOD CIO, 2013). The CIO outlined that APAN was the designated enterprise service for sharing unclassified information with multinational partners, NGOs, and other U.S. agencies (Office of the DOD CIO, 2013). Therefore FIST had the option to either discontinue its work with the DOD, or to receive a waiver for the period required to migrate to the pre-existing DOD solution (Office of the DOD CIO, 2013).

C. FIST SECURITY ASSESSMENT AND POLICY GAPS

1. Mobile Application and Platform Assessment

In an excellent analysis of FIST's mobile application *Gather* and mobile platform, Google's Android OS, VanAssche (2014) focused his examination on access protections, data encryption abilities, provisions for the secure storage of credentials, and the MDM controls. Through analysis of the access protection features, VanAssche (2014) determined that, for the Android platform, these features formed the lynchpin of the platform's security architecture. Therefore, circumventing the access protections allowed an attacker near total access to the device, while simultaneously negating or rendering irrelevant many of the other security features. Furthermore, VanAssche (2014) found that the only substantial protection the FIST mobile application afforded against a determined attacker stemmed from a complex password based authentication system. Finally, with regard to access protection, VanAssche (2014) revealed that the collection and storage methods of the *Gather* application were insecure since the *Gather* application

did not enforce or require the use of the built-in access mechanisms despite the platform's reliance on the access protection mechanisms as the basis of its security assumptions.

Next, VanAssche (2014) examined FIST's support for, and use of, various data encryption tools wherein he determined that the Android platform does indeed include "robust and extensible support for most modern encryption standards." What VanAssche (2014) also found was that despite the robust capability, the implementation encryption standards on the platform fell short in that individual application developers were free to specify which algorithms and modes their applications used. This freedom is problematic from a security standpoint because the FIST platform preserves support compatibility for algorithms and modes that are no longer considered secure (VanAssche, 2014). Distressingly, the default choices for many of the platform's encryption methods were the less secure methods, and thus VanAssche (2014) remarked that the application developer's selection of encryption methods completely subordinated the security of an individual application's use of the file encryption tools.

In order to determine how well the platform conformed to the policy set forth in DODI 8520.02, an examination of the platform's mechanisms for secure storage of credentials and other secret keys is necessary. VanAssche (2014) concluded that the Android platform offered only "limited support for the secure storage of shared secret credentials, such as symmetric encryption keys and account passwords, although it featured robust support for secure storage of PK cryptographic certificates." Indeed, VanAssche (2014) determined that the implementation of file system permissions and limited access provided the bulk of the platform's protection for shared secret credentials. While this feature would seem to conform to the existing PKI/PK policy, VanAssche (2014) found that these protections offered only a token defense, and could be defeated easily through the use of a super-user account on the device. Not surprisingly, Google has recommended the use of user-inputted secret keys, rather than reliance on shared secret credentials stored on the device itself for this very reason (VanAssche, 2014). With specific focus on the *Gather* application, while it met the security policy criteria on paper, in that it made sufficient use of the protected storage space provided by the OS for its sensitive data, VanAssche (2014) determined that this data was not protected by an

off-device secret key, and thus per the discussion above, remained vulnerable to exploitation through the use of a super-user account on the device.

A critical element of the system, and in accordance with the DOD Mobile Device Strategy, is the concept of security through MDM controls. VanAssche's (2014) examination of the platform revealed severe deficiencies. The platform documentation espoused extensive MDM controls, and touted that they could be incorporated into applications developed for the platform (VanAssche, 2014). Unfortunately, as VanAssche (2014) discovered, these controls were centered on enforcement of access protection, and therefore offered limited ability to restrict the use of the device or destroy carried data after the fact if the device were discovered to be lost or stolen. Given the substantial threat of loss or theft for a mobile device, particularly in a tactical environment, this shortfall represents a severe security shortcoming. Thus while conformance to the existing security policy appears to afford a degree of protection, in practice the emphasis on strong access protection within the security model framework of the Android platform results in the simple reality that the *Gather* application cannot implement the requirements because it did not incorporate any of the potential MDM controls (VanAssche, 2014).

2. Mobile Application Data Transport Assessment

In verifying how the application fit within the policy framework provided by DODI 8510.01 and DODI 8320.02, several issues and vulnerabilities emerge. VanAssche (2014) found that the mobile application relied on the default Android SSL cipher suite priority, and thus used a cipher with known and demonstrated vulnerabilities as its default data interchange encryption method. In addition to deficiency, review of the contents of the mobile application data interchange revealed the presence of two other significant security vulnerabilities. As VanAssche (2014) remarked, every instance of data upload carried out by the *Gather* application contained the username and password for the FIST system of the user, and worse yet displayed the data upload in plain text. This defect guaranteed that an attacker able to defeat the cryptographic protections of any of the data interchanges enjoys full access to the FIST system (VanAssche, 2014).

Additionally, as VanAssche (2014) annotated, the data interchange used only the transmitted username and password to authenticate the data session, and therefore did not require or make use of a mechanism to verify the validity or "newness" of a session. Simply put, this vulnerability puts data upload to the FIST system from the *Gather* application at risk replay attacks, regardless of whether or not the attacker was able to defeat or interfere with the inherent cryptographic protections of the data stream itself (VanAssche, 2014).

3. Analysis of Security Policy Gaps

Following review of the security policy literature and comparison with the vulnerabilities discussed above with regards to the FIST mobile application, platform, and application data transport, it becomes clear that current policy is in fact adequate in that it requires proper protections of the DOD Information Enterprise. How then, given the adequacy of the policy, can one explain the myriad vulnerabilities VanAssche (2014) noted in the system? The simple answer is that the policy provides high level guidance which is relatively easy to meet on paper when compared against the practicalities of testing system vulnerability against evolving threats.

D. CONCLUSION

The lessons learned from the case of FIST/Lighthouse are clear. Though the brainchild took two different routes to attempt to bring an asked for solution to the DOD, one government-owned and government operated, and the other contractor-owned and contractor-operated, neither has been wholly effective. Plagued by difficulties ranging from inter-programmatic disputes, to official policy concerning mandated use of existing enterprise solutions, FIST and Lighthouse's attempts to fulfill the originally intended purpose have fallen short. Of course, the DOD should rightfully seek to protect its networks and to prohibit untested and therefore potentially vulnerability-increasing systems from having carte-blanche access. However, the stymied efforts of FIST and Lighthouse also provide a sharp lesson to creative developers: the DOD is not the place for cutting edge smartphone-enabled software. In particular, the requirements for managing the complex network of stakeholders, organizational interfaces, and resistance

point to the increased likelihood of failure for any stand-alone of bottom-up innovations within the DOD (Roberts and Longley, 2013, 186–189). Those operating at the proverbial "pointy end of the spear," in other words the innovative junior personnel at the war fighting level, have at best a limited understanding of the larger policy, approval, and acquisition process which can take years to master and comprehend (C. Longley, interview with the author, July 29, 2014). In this sense, those best positioned to see the need and possibilities for the newest technologies are the least-suited to be able to do anything about affecting their implementation.

Most interestingly about the agonizing experience of Lighthouse and FIST is that Longley's initial idea in 2007, to use radio-linked smartphones to collect and analyze data from the field was novel at the time, and yet almost blindingly obvious at the time of this writing in 2014. Indeed, perhaps many of the hurdles FIST and Lighthouse faced were precisely due to the revolutionary nature of the concept. Certainly, in its initial stages Lighthouse found champions such as Lieutenant General John Mulholland whose "extensive field experience enabled him to immediately see its value and import" (Roberts & Longley, 2013, p. 187). Yet, proposing such a concept today would hardly need to receive such support from on high, as it is seemingly mundane and hackneyed. From a DOD Policy and Acquisition standpoint, designed to tackle projects such as next generation air to air fighter design and warship creation, it might be hard to imagine an idea which is only three to five years old having been ahead of its time. Yet, in the rapidly evolving field of smartphones and software it's an entire generation of difference: a generational divide which means the difference between cutting edge and common-place. In the world of military conflict, these small leads can disproportionately affect the outcome of an engagement. Balancing the requirements of GIG security while also incorporating technologies which afford a competitive advantage necessitates a review of the gaps in DOD policy and the policy formulation process.

E. SECURITY POLICY RECOMMENDATIONS

Prior to examination of the process by which the DOD makes security policy, which will follow in chapter four, this chapter will discuss those specific policy changes needed to accommodate secure smartphone systems such as FIST into the DOD.

1. FIST Policy Recommendations

From his comprehensive security analysis, VanAssche (2014) provided the following recommendations to address his specific identified vulnerabilities of the FIST system:

- Employ DNS WHOIS obfuscation to hide personnel and contact data
- Employ DNSSEC technology
- Remove specific identifying information from web server HTTP headers
- Remove OpenAtrium and Drupal identifying information in filenames and directories
- Remove OpenAtrium and Drupal miscellaneous text files unrelated to functionality from public directories
- Employ improved sanitization functions for *FusionPortal* data inputs
- Implement Android device management controls within *Gather* app that enforces complex password device access protections
- Ensure encryption algorithm and mode employed by *Gather* application does not contain cryptographic weaknesses
- Ensure *Gather* application secure data files are protected by an off-device secret key
- Override default Android SSL cipher priority list to ensure more cryptographically secure ciphers are used for data transport
- Standardize *Gather* application data upload format to the same used in the web application, including session authentication tokens and remove use of username and password for authentication of data transmission (VanAssche, 2014, p. 77)

It goes without saying that after correction of this initial list, further testing should be performed to determine the efficacy of the enhancement. Moving beyond FIST, a baseline of security features for mobile applications in general merits discussion.

2. Mobile Application Security Policy in General

Mobile application developers must understand and indeed question the underlying platform's security assumptions, and subsequently engineer applications to conform to those security assumptions, rather than assuming away risk by failing to investigate and match the two. Notably, as VanAssche (2014) attested, access protections, are a critical component of every mobile platform's security assumptions, and hence in order to be considered secure applications which store or rely upon sensitive data stored within the device must maintained the integrity of access protections.

Getting into the Design aspects of device and system creation, and as discussed earlier in this paper, mobile devices are frequently optimized first and foremost for, and indeed one of their principal appeals lies in, efficiency, rather than security (VanAssche, 2014). This simple truth means that the default settings in mobile platforms which support application development are generally not appropriate for a secure application. As such, these platform and system defaults must be examined in detail, tested, and often overridden in order to achieve total system security (VanAssche, 2014). Mobile device policy must recognize this fact, and explicitly mention the need to validate and test such defaults.

Finally, as mentioned previously, prudency demands that the theft or loss of a mobile device is all but assured. Applications, and the policy which guides their development, must therefore keep this reality at the forefront during development, and whenever possible, should not require the storage of sensitive data on the device. If such storage is necessary, protection mechanisms should rely on data stored the off the device (VanAssche, 2014).

3. DOD Policy Reform Recommendations

In noting that the existing policy was not inherently flawed, in that the nature of its language does indeed instruct taking adequate protection for mobile devices and their applications, this researcher does not intend to create the false notion that the policy is ideal. Given the relative vagueness of policy documents, in that they are designed to apply holistically to the broad range of the DOD IE, and as compared to the highly

specific, individualized, and time-varied nature of security threats to mobile devices, it seems there are two overarching solutions to better govern device and application development and implementation. Either policy must be so up-to-date and specific such that it covers all of the emerging threats in a timely manner as to allow the Acquisition process the lead time to develop modern products, or an entirely novel approach to development and testing must be implemented such that the vagueness of the policies is does not introduce risk or ambiguity.

It is beyond the scope of this research to delve into a conceptual structure for a new development and testing approach, and though this topic will be addressed in a later chapter, such an approach would require a reconfiguration of the acquisition process, the policy process, and how the DOD interacts with industry and other elements of the federal community. Within the DOD's control however, is the possibility to introduce changes in the policy formulation process such that specific policy might be created in a timely enough manner as to allow the acquisition cycle the necessary lead to develop modern and secure systems. It is to the redesign of the policy formulation process that this paper now turns.

IV. SIMULATION

This chapter will assess gaps in the current policy formulation process of the DOD by modeling the As-Is DOD Issuance process. The methodology for this chapter takes the issuance approval process from the DOD Issuances website (Department of Defense, 2014a) and inputs it into the Savvion business process modeling software application. Once the current process is modeled and gaps identified, this chapter will proceed to model a potential future process (To-Be). The results of the two simulations will be presented in chapter five and then analyzed in chapter six.

The Savvion process modeler is a "visual, easy-to-use tool that empowers [one] to design processes, run simulations, and store and retrieve processes from a central shared repository. To put it simply, people use Process Modeler to 'articulate the way they think' about their business" (Savvion, 2006, p. 5). The rationale for using Savvion's process modeler is that Savvion was rated by Forrester Research as one of the leading business process modeling vendors, the Savvion software was free to obtain, functions well as a stand-alone system, and comes with an easy-to-use tutorial which familiarizes a new user with the software quickly (Savvion, 2006, p. 2). The short learning curve and ease of use Savvion offers, coupled with multiple positive reviews placing it on par with other business process modeling software applications, made Savvion the logical choice for this research. Furthermore, Savvion provides its results in a format conducive to exportation into Microsoft Excel. Rapid transfer between the software's output and an excel spreadsheet is highly desirable as Excel comes standard within the Microsoft Office Suite common to DOD systems, and because the KVA output, discussed in chapter five, requires use of Excel. For a detailed explanation of how Savvion collects inputs, models them, and provides outputs, see Appendix F.

A. AS-IS POLICY FORMULATION PROCESS

In order to better understand the shortfalls of the current DOD policy formulation process, this research used the business process modeling software Savvion to produce a basic process flow. In order to keep the process simple, so as not to be overly bogged

down in detailing the current (As-Is) process, several assumptions were made concerning personnel involved, costs, work times. The key element in comparing the As-Is process to the To-Be (the future process to be discussed in the Recommendations Chapter) is consistency. Therefore, while the assumptions are likely not all-inclusive, so long as they remain the same, the relative scale of the costs and benefits will remain within the same orders of magnitude.

The current generic policy formulation process, as taken from the DOD Issuances Website (Department of Defense, 2014a), can be modeled as follows:

1. Process Flow

The process flow for a DOD Issuance occurs in five stages:

- STAGE 1: DEVELOPMENT. Draft the issuance and coordinate internally within component.
- STAGE 2: PRECOORDINATION. Get a precoordination edit from Directives Division (DD) and a legal objection review (LOR) from the Office of the General Counsel, DOD (OGC).
- STAGE 3: FORMAL COORDINATION. Coordinate with external agencies. Adjudicate and ncorporate external agency comments in coordination with OGC.
- STAGE 4: PRESIGNATURE. Send the final coordination package to DD for review and obtain a legal sufficiency review (LSR) from OGC. Also, obtain a security review from the Defense Office of Prepublication and Security Review (DOPSR).
- STAGE 5: SIGNATURE AND POSTING. Send the final issuance to DD for posting to the Internet.

There are multiple steps within each phase, which are now outlined in detail. The percentages listed at the end of each step represent the percent of issuances which must go through that particular step in the model.

Stage 1:

- Component - Assign a Number to the new issuance: 100% of all issuances.
- Component - Draft the Issuance: 100% of all issuances.

- Component – Determine External Coordination Requirements : 100% of all issuances.
- Component – Prepare the SD Form 106 to begin the routing process: 100% of all issuances.
- Stage 2:
- Directives Division – Precoordination Edit. This edit involves a subjective review, a technical review, and a review of SD Form 106: 100% of all issuances.
- Component – Incorporation of Directives Division edits. 100% of all issuances.
- Component – Requests OGC LOR. 100% of all issuances.
- Component – submits edited issuance to the DD for posting. 100% of all issuances.
- Directives Division – Post issuance to the portal. 100% of all issuances.
- OGC – Legal Objections Review. Percent Legally Objectionable 70%; Percent Not Legally Objectionable 30%.
    - If Legally Objectionable, Component revises the issuance.
- Component – Requests Formal Coordination: 100% of all issuances.

Stage 3:

- Directives Division – Post Issuance to the Portal: 100% of all issuances.
- External Agencies – Formal Coordination: 100% of all issuances.
- Component – Adjudicate Coordination and Revise Issuance: 100% of all issuances.
- Component – Request Presignature Review: 100% of all issuances.
- Stage 4:
- Directives Division – Presignature Review: 100% of all issuances.
- Component – Review the Issuance. 100% of all issuances.
- Directives Division – Post the Issuance to the Portal: 100% of all issuances.
- OCG – Legal Sufficiency Review: 100% of all issuances. Percent Legally Sufficient 75%; Percent Not Legally Sufficient 25%.
    - If Not Legally Sufficient, Component revises the issuance
- Component – Request DOPSR Clearance: 100% of all issuances.
- DOPSR – Security Review: 100% of all issuances.

- Component – Revision and Final Package Preparation: 100% of all issuances.

Stage 5:

- Office of the Secretary of Defense – Posting Review: 100% of all issuances.
- Office of the Secretary of Defense – Signature: 100% of all issuances.

Office of the Secretary of Defense – Dissemination: 100% of all issuances

2. Assumptions

- The DOD processed approximately 36 Directives in 2013. Therefore, for the purposes of this project we will assume a twelve month work period, and will input a new directive beginning every 10 days for a total of 36.
- Based off of the number of reviews and revisions, it is assumed that all of the Directives which reached the desk of the OSD were signed. In reality this is not the case, as some may need to go back for revision. As each revision would potentially require further Legal Sufficiency Review and possibly Clearance review, this research omitted this re-work loop in favor of simplicity.
- Other than for the SecDef and his Under Secretary, military pay scales were used for all other workers, including the OGC.
- All Directives which made it out of the internal component review would eventually be processed (i.e. none were declared unnecessary and scrapped during the process).
- Assumed Legally Objectionable Review Percentages (70/30) and Legally Sufficient Review Percentages (75/25).
- Each actor in this process has a scheduled amount of time to complete work on the issuance. This scheduled time differs markedly from the time required to perform the work. As such, an inbox for each actor (with a billed rate of $0) was created to account for this structural delay.
- Assumed two days (written as hours within the model to allow for faster run times) for the component to turn around revisions.

3. Employees and Pay Rates

The As-Is process entails several primary action agencies, each with an associated number of employees and hourly rates. As will be explained in the following section, to save time running the simulation eight hour work days were compressed into one ‘hour’ of simulation. As such, a daily pay rate for an employee is translated into an hourly

charge when entered into the model (see Appendix F for how this information is entered). Furthermore, the pay rates are designed to portray relative costs of the model as compared to other alternatives, and thus the personnel costs include only base pay rates, and do not include additional benefits such as housing and subsistence allowances. Of particular note is that the employees and hourly rates are estimates, and are reflected below, and the theoretical basis for adding in costs stems from the previous KVA discussion as a means to translate utilization of human capital.

a. Component

At the component level, an action officer is an O-4. To obtain signatures or prior to routing to the Directives Division requires an O-5 review and an O-6 approval. Therefore, the O-4 does 85% of the work, the O-5 does 10% and the O-6 does 5%.

The composite rate per work day assumes a 40 hour work week, for 244 work days (which is the number of non-weekend work days minus the expected days off military personnel typically receive for federal holidays [16]) a year.

For simplicity, it is assumed all officers are relatively junior in grade, therefore their monthly pay will be assumed to be as indicated by Figure 9.

Level	Monthly	Annual	Daily Rate	Weighted Avg
O-4 (over 10)	6,593.10	79117.2	324.2508197	275.6131967
O-5 (over 16)	7,974.00	95688	392.1639344	39.21639344
O-6 (over 20)	9,625.20	115502.4	473.3704918	23.66852459
				338.4981148

Figure 9. Component Hourly Rate Calculation

Thus one sees that for the component, their cost is roughly $338.5 per work day. As previously mentioned, such that the modeling software works more quickly and cleanly, the translation of work days into work hours was used. Translating the rate for one work day into the model, *this researcher will charge at $338.5 per "hour" for the component.* This conversion will be used for all subsequent pay rates in that one work days' worth of weighted pay will equate to one hourly charge in the model.

b. Directives Division

It can also be assumed that the work at the directives division is again done primarily by a mid-grade O-4 and that a mid-grade O-5 reviews the directive briefly following the O-4's edit. Therefore, as depicted in the weighted average of Figure 10, it will be assumed the O-4 does 90% of the work, and the O-5 does 10% for this actor.

Level	Monthly	Annual	Daily Rate	Weighted Avg
O-4 (over 10)	6,593.10	79117.2	324.2508197	291.8257377
O-5 (over 16)	7,974.00	95688	392.1639344	39.21639344
				331.0421311

Figure 10. Directives Division Hourly Rate Calculation

Thus the charge will be $331 per hour for the Directives Division.

c. Office of the General Counsel

The model will assume that the Legal Review is conducted primarily by an O-5 with O-6 oversight. Therefore the O-5 will do 85% of the work, and the O-6 will do 15%. Using the same scales as before the pricing for the Office of the General Council (OGC) is shown in Figure 11:

O-5 (over 16)	7,974.00	95688	392.1639344	333.3393443
O-6 (over 20)	9,625.20	115502.4	473.3704918	71.00557377
				404.344918

Figure 11. Office of the General Counsel Hourly Rate Calculation

Thus the OCG rate is charged at $404.34 per hour.

d. DOPSR

It will be assumed the work at the security office is done primarily by an O-4 with some supervision from an O-5. Their pricing therefore will be identical to the Directives Division. *Thus the model will charge $331 per hour for the DPOSR.*

e. Office of the Secretary of Defense

A valid assumption is that the secretary himself does not do the majority of the work in reviewing the directives that come into his office, and that he has senior staff doing almost all of that work. It can be assumed then, that an O-6 does 80% of the work in the OSD, an O-8 does 10%, the Under Secretary for Defense Policy (USD (P)) will do 5%, and the Secretary himself does about 5%. Figure 12 displays this pricing model.

Level	Monthly	Annual	Daily Rate	Weighted Avg
O-6 (over 20)	9,625.20	115502.4	473.3704918	378.6963934
O-8 (over 26)	13,647.30	163767.6	671.1786885	67.11786885
USD(P)	13,775.00	165,300	677.4590164	33.87295082
SecDef	16641.67	199,700	818.442623	40.92213115
				520.6093443

Figure 12. Office of the SecDef Hourly Rate Calculation

Thus the OSD will charge $520.6 per hour.

f. External Agencies

By external agencies, we mean other components as well as other agencies with the DOD (DIA, DISA, etc.). We will assume rank equivalence with the drafting component, and as such, the hourly rate is the same *$338.5 per hour as charged for the component.*

4. As-Is Process Model

The As-Is process was put into the Savvion modeling simulator. Of note, in order to ensure the software did not take an inordinate amount of time to run a simulation, a simple conversion was made in that an entire eight-hour work day was modeled as one hour. Thus a work time of five hours in the Savvion model represents five, eight-hour work days. As an additional note, due to the scheduled delays in the timeline per Table 3 of DOD instruction 5025.01 (Department of Defense, 2013a), zero-cost "inboxes" were added to the model to account for the delays without adding massive work time. In other words, while the OGC might have ten days to provide the Legal Objection Review to the

component, the OGC does not in all likelihood perform ten, eight-hour days' worth of work on the issuance. The no-cost inboxes account for the time incurred while allowing manipulation of the actual time spent on the legal review. Figure 13 shows the simplified As-Is model.

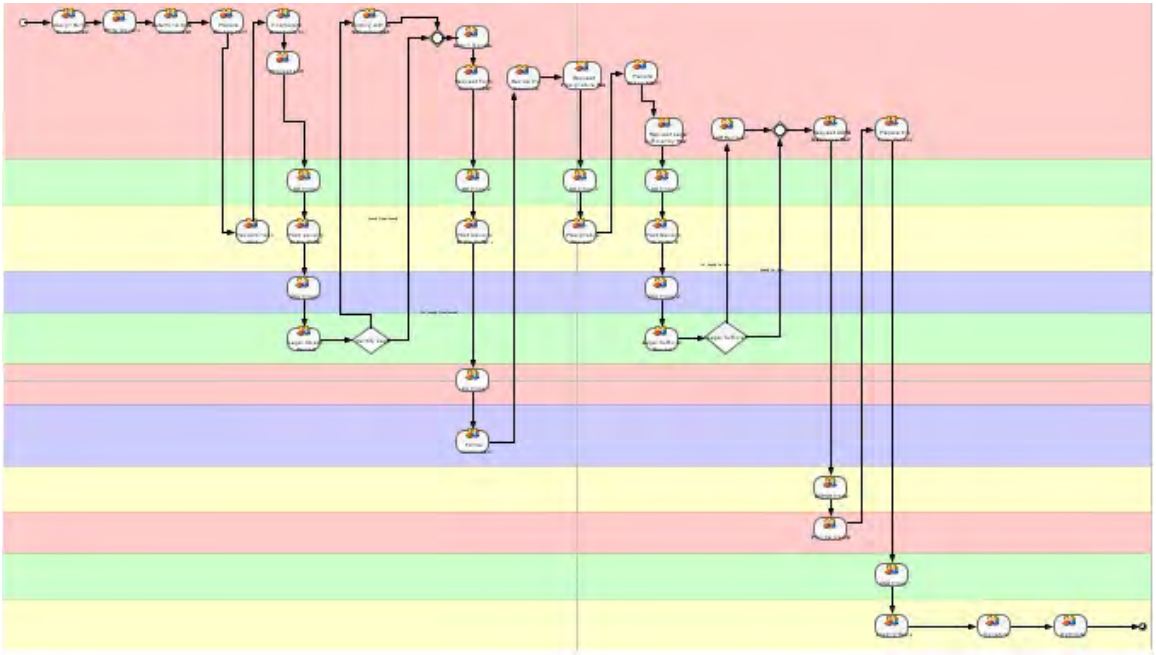

Figure 13. As-Is Savvion Process Model

What becomes immediately clear is the hierarchical nature of the process flow wherein only one actor works on an issuance at a time, and where all changes and edits must go back to the originator to be enacted. While the simulation is no doubt somewhat simplified from the actual process, it is hard to believe indeed that simplification would *lengthen* the issuance process. Therefore, with respect to the fit between current the policy formulation process and the evolving technologies inherent in smartphone and mobile technologies, it becomes obvious that no matter the type of policy, be it security or otherwise, the hierarchical model breaks down when rapidity is desired. Indeed, if the hierarchical model was the pinnacle of fit for an Industrial Age organization, the requirements for using mobile devices and the fundamental mismatch we witness between our policies and what they govern should convince us that we are in the throes of

transition to an Information Age organization. In that sense, what is required as we move forward is the use of collaboration and design. Indeed, this type of structure represents the ideal target for BPR and Design Thinking (for a detailed discussed of BPR and Design Thinking, see Appendix E).

B. TO-BE POLICY FORMULATION PROCESS

Taking the theories of BPR and Design Thinking into account, the policy formulation change effort sought to achieve time and cost savings within the process, while making it more collaborative and thereby more responsive to the turbulent environment of software and mobile devices. The process redesign goals are as follows:

1. Business Process Reengineering Goals

- Reduce wait time by at least 90%, ensuring that each activity with wait time is reduced by at least 50%.
- Reduce duration by at least 25%.
- Reduce utilization for OGC, Component and Directives Division by at least 50%.
- Increase throughput from 36 issuances per year to 50 issuances per year (or higher).

Of note, reducing costs is not in the list of BPR goals. This is intentional and measured. Certainly the government always seeks to reduce costs in everything that it does, and this has never been truer than in eras of fiscal constraint. However, reducing cost cannot and should not be a goal of this change effort because of the slippery and elusive nature of that goal. In other words, even if the BPR reduced costs by 50%, could the argument not be made that the government would still prefer to have reduced it by 75%, or even 90%? As such, the extreme of this goal suggests that in fact cutting costs is easy: eliminate the entire process altogether; or even more radically, cut all government costs by eliminating the government! This somewhat pedantic argument is presented merely to explain that while surely attempts to reduce costs are necessary and should be encouraged, cost reduction cannot be one of the primary goals where government is concerned since from an existential perspective one must accept that the cost of doing business, in this case of processing and publishing policy, is a necessary evil, and

certainly better than the alternative (accepting massive risk and having complete dis-unity of effort by publishing nothing at all).

2. Future Process (To-Be)

In order to achieve such drastic process improvements, it becomes clear why BPR is required, and why Lean or Six Sigma improvements, also known as continuous process improvements (CPI), will be insufficient. In other words, radical redesign of the process is the only means which can accomplish the assigned goals. In this instance, the underlying theoretical construct for the redesign lay in the field of design thinking, which focuses heavily on collaboration, creativity, rapid prototyping, and empathy with the end user (for a full discussion of the design thinking process, see Appendix E). At the same time, it is understood that to achieve a realistic process, the legal and political machinery which regulates the DOD cannot be assumed away (i.e. one cannot presume the entire DOD structure would be modified to achieve process improvements for releasing issuances). In this manner, and in accordance with best practices and research from the field of Change Management, successful adoption and implementation of the change effort necessitates that only certain aspects of the process be redesigned.

Taking design thinking into account, one notices the completely sequential nature of the process. DOD Issuances move from one stove-piped piece of the hierarchy to another in a logical, deliberate fashion. Each entity had time to review it, make edits, and then send it back to the component for revisions before the issuance moved on to the next stage in its life cycle. It was precisely this "sequentialism" that the BPR effort sought to destroy as it adds needless delays and places considerable burden on the component in terms of revision.

The To-Be process incorporates the collaborative emphasis from design thinking. While the component still writes the initial draft of the issuance, several things change. First, the goal of writing an issuance is not to "get it right" the first time, but rather to provide a template off of which the collaborative process can begin. Thus the component will spend a shorter time drafting the issuance.

Next, there is no need for the Directives Division to pre-edit the issuance for a five day window following which the Directive Division must post the issuance to the portal. Under a collaborative model, the whole objective is the push the issuance into the portal as rapidly as possible to allow the creativity of the collective (i.e. all concerned stakeholders) the maximum time to interact with it. Thus, the component can post the issuance, and rather than the issuance being pulled off and then re-posted each time, once posted to the portal, the issuance will remain posted. In the same manner as a GoogleDoc, version control will be accomplished through the time-stamping of edits such that the issuance is modified in real-time. Furthermore, an RSS feed would alert each of the various stakeholders to the presence of a new issuance on the portal. This removes the need for the component to determine formal coordination requirements as well as the need to request formal coordination. The "Alert" method is preferable because rather than rely on the component to estimate which stakeholders might care to be involved (this was the "Determine Formal Coordination Requirements" step from the As-Is), involvement is assumed from all stakeholders (as naturally all would have access to the portal), and those who have no stake can simply "opt-out" by not making any modifications.

What then follows is a period of intense and simultaneous collaboration. This period would be messy as organizations (to include legal and the directives division which would act as overseers to ensure the process stays on track and within its scope) modify and debate the various merits of the issuance. Such contentiousness is desirable as it bypasses the formality of non-concurrence in that each entity is *encouraged* to make modifications rather than simply accept or reject the proposed issuance. This stage is kept necessarily short so that the stakeholders maintain focus on the issuance at hand.

Following the collaborative stage, the component works to clean up the issuance, and the more scripted, formalization of the issuance takes place. The component will make any touch ups and request a final, formal legal review. The OGC will perform a single legal review, in place of the previous Legal Objection Review and the Legal Sufficiency Review. The logic for a single review vice two is that the OGC monitored the issuance development and provided feedback throughout the collaborative stage.

Thus only a single legal review is required, and that on a reduced timeline. In similar fashion, the DOPSR performs its security review as before, but on a reduced timeline given that they were also involved during the collaborative stage.

Finally, the Office of the SecDef performs its review, signs, and disseminates the issuance. As previously mentioned, since the structure of the DOD will not change to accommodate this one process, the Office of the SecDef's interaction will remain somewhat hierarchical and sequential to ensure adequate oversight and to remain within the framework of Executive and Congressional legislation. Finally, the last modification made was to increase the number of personnel at the component and OGC from one each to four and three, respectively.

Thus the To-Be process would look more like this:

Stage 1:

- Component – Assign a Number to the new issuance: 100% of all issuances.
- Component – Draft the Issuance: 100% of all issuances.
- Component – Post Issuance to interactive web Portal

Stage 2:

- Directives Division, OGC, DOPSR, and External Agencies – Input and Editing. 100% of all issuances
- Component – Collation of edits. 100% of all issuances.
- Component – Requests OGC Legal Review. 100% of all issuances.
- OGC – Legal Review. Percent pass review 75%; Percent fail review 25%.
- If revisions required, Component revises the issuance.
- Component – Requests DOPSR Clearance: 100% of all issuances.

Stage 3:

- DOPSR – Security Review: 100% of all issuances.
- Component – Revision and Final Package Preparation: 100% of all issuances.

Stage 4:

- Office of the Secretary of Defense – Posting Review: 100% of all issuances.

- Office of the Secretary of Defense – Signature: 100% of all issuances.
- Office of the Secretary of Defense – Dissemination: 100% of all issuances.

3. Additional Assumptions (for the To-Be Model)

- A new portal might have to be created that allows for interactive, real-time modification to issuances
- Stakeholders have designated personnel to monitor the issuances RSS feed and to provide input and edits absent formal coordination requests

4. To-Be Process Model

Based off of the goals and assumptions listed above, the To-Be Model is focused on enabling collaboration rather than stove-piping work between organizations. While to the lay-viewer the models might not look entirely different, the key area to note is the one with the red circle around it in Figure 14. It is in this area that the period of intense collaboration occurs. Comparing the As-Is with the To-Be models one notices that after the collaborative phase the models look relatively similar. Again, as described previously and in accordance with change management theory, the latter half of the To-Be process was left hierarchical to both temper the strong reaction against the change effort and in recognition of the fact that the entire structure of the DOD is unlikely to change in order to ameliorate the issuances process.

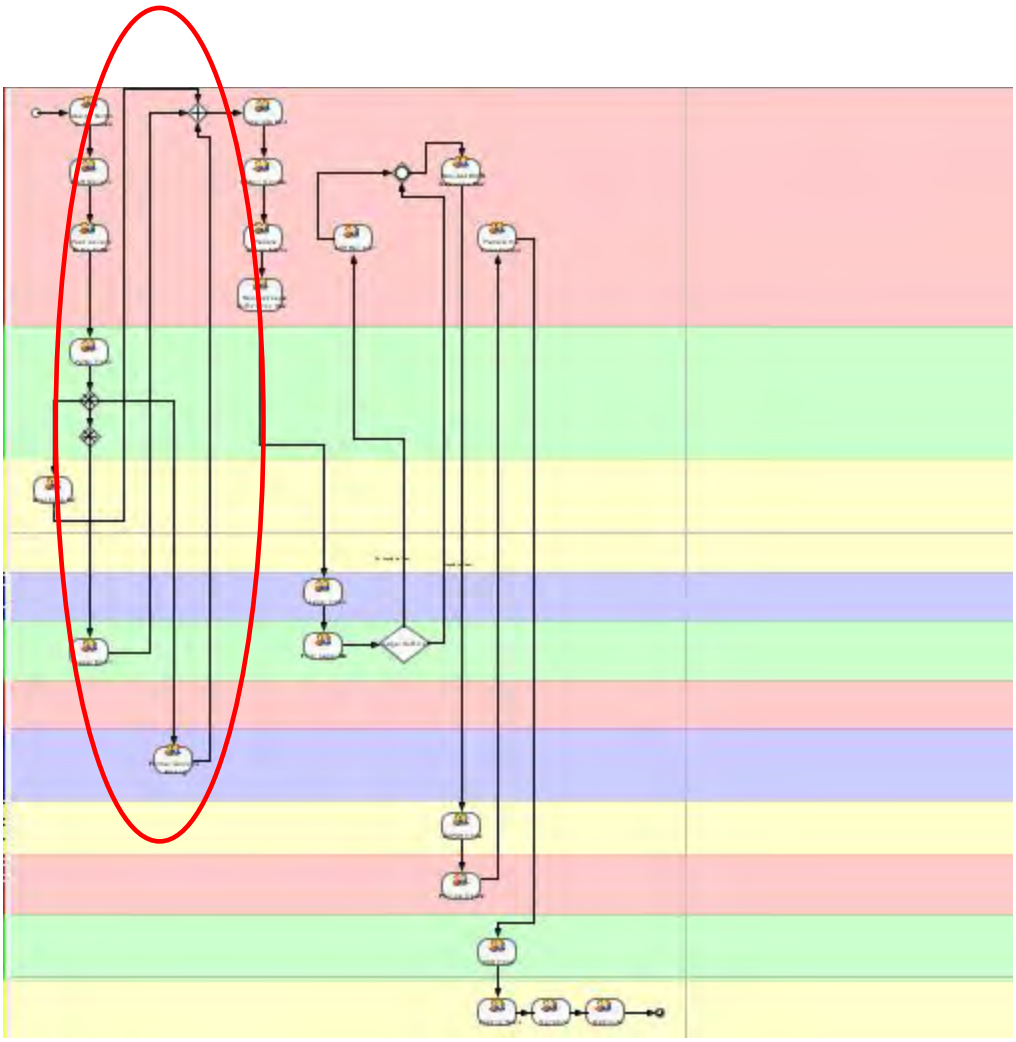

Figure 14. To-Be Savvion Process Model

C. SUMMARY

This chapter presented two models, an As-Is simulation of the current DOD Policy-making process, and a To-Be process, and relied on the Savvion process modeler tool to build and simulate them. The impetus for radical process redesign can be found in BPR theory (as described in Appendix E), major difference between the two models stemmed from the theoretical backdrop of rapidly iterative collaborative creation contained within Design Thinking (also discussed in Appendix E). The following chapter will discuss and compare the results from the two models.

V. SIMULATION DATA AND RESULTS

This chapter will discuss the results obtained from simulating the As-Is and To-Be models of the DOD policy formulation process. The full tables of the results can be found in Appendices A through D, and therefore only results of import will be elucidated in the following discussion.

A. AS-IS SAVVION OUTPUT

Running the As-Is simulation for 36 issuances (the number published by the DOD in 2013 according to the DOD Issuances Website), yields the data in Appendix A. Several results are of particular note. First, the total duration of 703:15:00 translates to 703.25 work days to complete the 36 issuances. More simply put, the current DOD Issuances process holds the potential to require two years' worth of work days to accomplish a single year's worth of work. A second look at Appendix A shows the "Waiting Time" column is nearly entirely red, representing massive delays. Since only one actor may work on an issuance at a given time, and assuming that an office does not find or task extra people to work on issuances, given that they have myriad other tasks to accomplish, massive delay builds up on issuances in the queue while entities wait for a previous issuance to be published. Lastly, under the "Utilization" column of the "Performers Queue Length and Utilization" section, one also notices the high utilization rates for the component and the Directives Division (91.57% and 70.17%, respectively). While at first glance one might think high utilization represents efficiency, taken into context that the actors have other tasks, it becomes readily apparent how harmful high utilization can be. In other words, if a person at the component spends 90% of his/her time processing issuances, they do not have time for anything else, to include going to meetings, or conducting annual training.

Other aspects of the process as modeled are in line with expectations. For example, the Office of the SecDef is shown at approximately 11% utilization. Far from representing inefficiency, this value is if anything too high. One would not expect the

Secretary of Defense to spend more than 10% of his time reviewing DOD Issuances, particularly given his duties on the National Security Council.

B. AS-IS KVA OUTPUT

In an effort to measure the utilization of human capital the work times and associated costs from the Savvion output in Appendix A were translated into a measure of knowledge value added (KVA) using principles from the theory of KVA found in Appendix E. The most stirring results from this output can be found in the utilization percentages. The directives division utilization came to 195.2%, while the component's utilization was a startling 1036.4%. In other words, it should come as no surprise that under the current model it takes over two years to accomplish one year's worth of work, since the main actor responsible for generating and doing most of the work on an issuance (the component) is supremely over-worked. Similarly the main interface between the component and the larger policy-making process (the directives division) is also over-utilized, which further contributes to the delays noted in the As-Is Savvion output.

To determine the generated value to the process of the human capital in the directives division and the component, one can divide the revenue generated by an activity by total revenue generated in the process (column R) in Appendix B. Doing the same (dividing the cost for an activity by the total cost of the process) for costs produces column S of Appendix B. These two columns on the far right side of Appendix B provide a side-by-side comparison for the value and cost of an activity relative to the entire process. For instance, the comparison shows that the "Prepare the Final Package" step generates nine percent of the value in the process, and comprises four percent of the total cost. Rather than delve into minutiae for each step in the process, the critical comparison is in the revenue and costs associated with the two over-utilized actors: the directives division and the component, particularly as compared to lesser used actors, such as the OGC. By adding up the revenue and costs percentages from columns R and S for each actor, the As-Is revenue versus cost is illuminated by Figure 15.

Actor	Value	Cost
OSD	8%	1%
OGC	19%	5%
DD	10%	14%
DOPSR	1%	1%
Component	60%	76%
Externals	2%	4%

Figure 15. As-Is KVA Value versus Cost

What becomes immediately clear is that the component and the directives division produce 70% of the value, and incur fully 90% of the total cost. By contrast, the Office of the General Counsel generates almost 20% of the revenue for only 5% of the total cost. Therefore, it is not surprising that the total return on knowledge (ROK) as compared to the total cost to benefit ratio, found in columns P and Q, respectively, is comparatively low at 32% and 31%, respectively (essentially 1:1).

C. TO-BE SAVVION OUTPUT

Following the redesign of the policy formulation process shown in Figure 14, the Savvion output produced the results shown in Appendix C. Most notably, whereas the duration in the As-Is model was over 703 days for one year's worth (36 instances) of work, the To-Be model took only 522 days to process two years' worth (72 instances) of issuances. Similarly, despite the doubled workload, the total cost for the To-Be model was only $409,294.8, as compared to the $ 573,632.21 for the As-Is model. Also of note was the elimination of wait time in the To-Be model. Finally, the utilization percentage for the component was reduced from 91.57% in the As-Is to 33.6% in the To-Be model, while the directive division's utilization was reduced to 6.89% from is As-Is high of over 70%.

D. TO-BE KVA OUTPUT

The KVA results from the To-Be simulation can be found in Appendix D. Notable results are the realignment of total activity time in the component from 1036.4% to 37.1%, and for the directive division from 195.2% to 6.9%. The OGC saw a reduction in total activity time from 54% to 32.2%, whereas the Office of the SecDef's

activity time increased to 20.7%. Significantly, Figure 16 displays the changed value versus cost generation (using the same process as generated Figure 15 above).

Actor	Value	Cost
OSD	14%	9%
OGC	34%	34%
DD	2%	2%
DOPSR	1%	8%
Component	45%	43%
Externals	4%	4%

Figure 16. To-Be KVA Value versus Cost

Lastly, and perhaps most significantly, the ROK versus the cost to benefit ratio improved by an order of magnitude to 128% and 8%.

E. RESULTS OF THE POLICY FORMULATION CHANGE EFFORT SIMULATION

Comparing Appendices A and C yields the following results as compared with the BPR goals introduced in chapter four:

- Reduce wait time by at least 90%, ensuring that each activity with wait time is reduced by at least 50%.
    - Overall wait time has been reduced by 100%, largely due to the "portal" style of issuance creation and addition of minimal personnel in two key areas: The Component and Office of the General Council.
- Reduce duration by at least 25%.
    - Duration was reduced from 703.25 days to 522.25 days, or a total percentage of 25.3%.
- Reduce utilization for OGC, Component and Directives Division by at least 50%.
    - OGC utilization was reduced by a total of 41%, Directives Division was reduced by 97%, and the Component utilization was reduced by 96%.
- Increase throughput from 36 to 50 (or higher).
    - Actions per year were increased from 36 to 72, surpassing the 50 action desired threshold.

F. SUMMARY OF RESULTS

This chapter presented and compared the results from the two Savvion models contained in Appendices A through D. Overall, the To-Be model met all of its BPR goals. The change effort reduced total duration by 25% and achieved roughly 30% cost savings while concomitantly eliminating wait time and improving percentage utilization for the directives division and the component by over 95%, in spite of a 100% increase in the number of issuances processed. The next chapter will analyze the reasons for such dramatic process improvement in light of the original BPR goals.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. POLICY PROCESS ANALYSIS

A. GENERAL ANALYSIS

Regarding the accomplishment of the BPR goals, there is room for discussion and analysis on why the change effort achieved such drastic results. Therefore, each improvement will be addressed in turn.

1. Reduction of Wait Time

In the To-Be model wait time was entirely eliminated. This meant that no issuance sat in an inbox waiting for an actor to take action on it because that actor was already working on an earlier issuance. In short, previously identified bottlenecks at the component and the Directives Division were neutralized.

2. Reduction of Duration

The reduction of bottle necks and wait time, and the simultaneous nature of the collaborative revision process introduced in the To-Be model, improved the duration to process an increased number of issuances markedly. In this sense, the principle of the design process to fail early to achieve success sooner is precisely what allowed the model inputs for the collaborative stage to be more rapid than in the As-Is model. By introducing more freedom, and more actors (via the External entities), a more comprehensive and more complete issuance is realized earlier in the process.

3. Reduction of Utilization

Naturally the reason for the reduction in utilization of the directives division is obvious: the division was all but eliminated in the To-Bo model and replaced by an interactive web-portal approach to policy-making. This interactive approach is also the reason behind the reduction in utilization for the component. In the As-Is model the majority of the work, such as writing the issuance, coordinating with external entities, editing, submitting for reviews, re-editing, and preparing the final package, fell to the component. In effect, the component did all the leg work to create the issuance, and then had to do all the work if some other entity disagreed with something or required changes.

The directives division was acting as a middle man in this whole exchange, and thus more work (particularly for the component) was generated purely by its existence. In moving to a more collaborative process via the To-Be model the onus to make changes falls increasingly on the stakeholders collectively, rather than a single point of failure: the over-worked action officer at the component. Similarly, since the OGC is involved earlier in the process as well, items which would likely be legally objectionable or be cause for legal insufficiency are addressed earlier, which translates to reduced time spent in legal review. Again, it is the collaborative nature and early involvement of the stakeholders which provides for this improvement.

4. Increased Throughput

The reduction in wait time coupled with the decreased utilization made for increased throughput in the To-Be model as compared to the As-Is. Indeed, doubling the number of actions taken while also reducing the total duration by over 25% is a result with which any organization could be satisfied. However, this is not to say the DOD should produce more issuances just because it has the potential to do so. Rather, the implication is that due to the decreased time, decreased utilization and increased rapidity with which a given issuance might be produced, the policy formulation process under the To-Be model would actually be able to keep pace with cutting-edge technology. This responsiveness is the true value of the To-Be model over the As-Is model. As discussed in the FIST/Lighthouse case study in chapter three, it is unreasonable to expect contemporary policy to remain valid with every advancement in technology, especially given the pace of change in the information age. Thus, the goal should be a responsive policy formulation process which can produce prudent policy guidance, based on relevant stakeholder input, in such a manner as to encourage the proliferation of novel ideas, and facilitate their rapid creation, adoption, and implementation into the force. Nowhere is will the effect of such rapid incorporation be more keenly felt than at the proverbial “tip of the spear,” the ground combat forces.

5. Reduced Costs

While reducing costs was not one of the original BPR goals, the change effort also realized cost savings. Though counterintuitive, the addition of personnel to the OGC and the component actually reduced total costs through the elimination of wait time. Additionally, the implicit addition of personnel to the process via increased stakeholder participation (identified in the more substantial involvement of external actors) also serves to keep costs down in much the same manner.

B. IMPLICATIONS FOR ADOPTION OF SMARTPHONES AND ASSOCIATED TECHNOLOGIES

By simulating the process whereby policy is drafted this research aimed to make the policy formulation process more inclusive of myriad stakeholders and more reactive to rapidly evolving situations which require published policy. As discussed in previous chapters, use of smartphone technologies, and in particular at the tactical level wherein network security is critical to protecting lives and insuring mission success, is a prime example of one such situation. Marines will go to just about any length to accomplish their mission. It is one of the hallmarks of the Marine Corps that its personnel will give that last full measure of devotion in order to succeed. It also means that bringing new technologies into ground combat units requires clear and up-to-date policy to govern their use. As presented in chapters two and three, despite the identified need for the technologies and encouragement for their use form the highest levels of the DOD, and as the case study of FIST and Lighthouse attested, there remain a plethora of concerning security gaps which should give cause for pause before tens of thousands of Marines are equipped with and allowed to use these systems in combat. The solution identified in this research was to expedite and make more comprehensive the policy which governs these systems on the assumption that such policy, in contrast to the technically correct but overly generic and insufficient contemporary policy, would thereby better protect the networks and lives of the troops.

At the conceptual level the two simulations represent a move from a more Industrial Age policy-making process, driven predominantly by the needs of the

hierarchy, to an Information Age approach driven by the COI and underwritten by collaboration. The improvements to the process as identified in chapter five and assessed earlier in this chapter are not an indictment of the As-Is model. Indeed this model has performed its function admirably in the past. However, the current process was not designed with the realities of the Information Age in mind, and the process is deliberately tightly controlled, and intentionally non-responsive as a means to ensure total hierarchical oversight. The gains realized in the To-Be model are possible through the advent of web-enabled interactive, real-time portals that permit collaborative policy creation among the various stakeholders. This process is at once both more fluid and reactive to changing situations as well as more rapid. Indeed if any terms could be used to describe the Information Age they would be interconnectivity, fluidity, and rapidity. The DOD needs such a process to ensure unity of effort across its many functions, of which its IE is certainly one of the most critical.

C. IMPLEMENTING THE TO-BE PROCESS IN THE DOD

Based on the changes to the policy formulation process proposed in chapter four, the true challenge in realizing a more responsive process is implementing it within the DOD. As discussed, the heart of the To-Be simulation was the collaborative web portal which allowed simultaneous real-time feedback, correction, edits, and review. Software applications such as SharePoint or Blackboard permit this type of interaction from a technological standpoint. Indeed, the decision to base the To-Be model around such software is a direct reflection of this technical reality. Rather, as the field of change management discussed in Appendix E suggests, the primary obstacle to a more collaborative process will be the physical organizational hierarchy of the DOD and its organizational culture. The necessity to be inclusive vice exclusive in the design and review process is anathema to the hierarchical nature of DOD development, review, and approval.

In order to keep the change effort to a manageable scope, such that it would not be rejected at face value upon initial introduction, large parts of the policy formulation process would be left unchanged. The OGC, DOPSR, and SecDef would retain their

responsibilities and authorities for review and approval, albeit they would be engaged in the process earlier. The directives division would not be wholly eliminated, but would be downsized and act in a more advisory and review capacity rather than as a middle man. Retaining these elements of the previous process serves to mollify those elements of the organization which might react most vehemently to the change on the fear that they were losing influence and power.

The next obstacle to tackle would be the inclusion of not only other DOD and Federal entities but players from the larger community of interest. An open web portal, wherein invitations are extended to stakeholders from the commercial and business sectors, as well as the academic and research oriented sectors, represents a major shift in ideological viewpoint for the DOD. As Kotter (2002, Kindle location 375) suggested, of the many factors required to spur an organization to accept change, the DOD needs to feel the sense of urgency regarding reformation of its policy process and would then need to see short-term successes. In that vein, perhaps the urgency to reform the process writ-large does not yet exist, since the DOD publishes many policy documents which are not tied to rapidly advancing technology. However, as illustrated in chapters two and three, the DOD policy process is significantly out of sync with smartphone systems, given the strategic guidance which advocates their adoption as compared to the stalled efforts of the types of systems asked for, in this case FIST and Lighthouse. To that end, this research recommends amending the policy formulation process specifically for network and software-related systems for which rapidity of publication can be the difference between cutting edge and obsolescence.

The short-term successes which are critical to a successful sustained change effort, the new DOD policy formulation process might be applied to systems already in existence, such as FIST and Lighthouse. Enabling these all-but-stalled systems to join the DOD IE following a rapid collaborative policy-making process would provide the DOD an asked-for capability in a timely manner, while still affording the COI the time to conduct extensive review on a real system, rather than one in development and testing. In witnessing the speedier yet judicious incorporation of novel technologies, stakeholders

in the DOD policy-making community might be better inclined to formally adopt an expedited policy formulation process for networks and software.

D. CONCLUSIONS

Overall, the results of the change effort were successful at the theoretical level, and significant time savings were achieved in conjunction with a 100% increase in throughput. Moreover, despite the addition of personnel, the changes achieved cost savings due to a drastic reduction in wait time. The true difficulty in effecting this change effort would be implementing it within the DOD, as an inherently hierarchical organization would have some difficulty embracing a less structured and more collaborative process for making policy. It is with that hierarchical structure, history, and culture in mind that the full discussion of change management was included in Appendix E. To that end, and as mentioned previously, this researcher recognized that the entire DOD structure would not be modified around the issuances process. Therefore, the more formal reviews leading to the SecDef level approval were left untouched in an effort to appease some of the discontent which might stem from radical change and make acceptance of the change effort more likely, while the change effort would be directed at lower levels of the bureaucracy.

VII. SUMMARY, CONCLUSIONS, SUGGESTIONS FOR FUTURE RESEARCH

A. SUMMARY

This research began by introducing the risks involved in the incorporation of secure mobile technologies within tactical ground combat units, such as loss or theft of the device, risks in the supporting architecture, and risks in data transport. Following discussion of both the new technological capabilities smartphones offer as well as vulnerabilities to the force which these capabilities bring with them, this research then broadly outlined uses of smartphone technology within tactical ground combat units in both humanitarian assistance and counterinsurgency scenarios. Having taken the premise of incorporation of smartphones into tactical units as a given, this research discussed implementation methods available such as Lockheed Martin's MONAX and Oceus Network's Xiphos system.

With the background case for smartphones, both good and bad, presented, this research turned to a discussion of existing policy. Starting with top-level DOD documents, such as the Mobile Device Strategy from the DOD CIO, this research examined successively more detailed policy documents. Taking into account guidance from senior leadership in the Marine Corps, and the priorities of the Commandant of the Marine Corps, this research surveyed the current USMC Vision and Strategy, the MAGTF 2012 C2 Roadmap, and the USMC Commercial Mobility Strategy to assess how USMC leadership sees smartphones fitting into the Marine Corps Information Enterprise (IE).

Digging a level deeper, this research conducted a review of existing DOD security policy, with the understanding that USMC security policy overwhelmingly falls within the scope of larger DOD directives. A range of security policy directives and initiatives were examined, and the research covered broad topics such as cybersecurity to those with narrower scope, such as PKI and PK enabling.

Reflecting the improvement-oriented nature of this research, this research presented the case study of FIST and Lighthouse at the Naval Postgraduate School to demonstrate a real system which has been impacted by current policy, and whose adoption might be expedited through an improved policy process. Through the lens of this case study, this research tackled the analysis aspect of smartphone security, and first sought to determine if the existing security policies, as written, contained shortfalls which created vulnerabilities.

Following this discussion, the research proceeded to assess the current policy formulation process to again determine shortfalls in the process which might introduce risk. The final portion of this research focused on providing recommendations to address the gaps and shortfalls identified in the analysis section as well as suggest a means by which a new policy formulation process might be introduced into the DOD.

B. CONCLUSIONS

Based on the work mentioned above, this research offers several conclusions regarding the incorporation of secure mobile technologies within Marine Corps tactical ground combat units. First, it is clear that the effort to incorporate such technologies is two-pronged, as both senior leadership and troops at the lowest levels are keen to take advantage of the benefits such technology affords. Second, as with any rapidly advancing technology, the likelihood of introducing vulnerabilities is inherent in their very adoption. With these two conclusions in mind, it becomes clear that the objective for the successful incorporation of needed smartphone capabilities down to the lowest tactical levels becomes risk mitigation and minimization.

As they stand now, current security policies are sufficiently vague as to allow them to remain the guidelines and framework for security systems, but inadequately detailed for use as a blueprint when building a secure device. In other words, while security policy requires developers to address the right topics, the policies do not, and this researcher argues cannot, list out the vulnerabilities to test or every software configuration to avoid. The issue then becomes whether to demand more granularity be included in existing security policy, or require an entirely novel approach to the

acquisition development, testing, and evaluation process. As previously discussed, it is well beyond the scope of this research to delve into reforming the Federal Acquisition Regulations, and hence this research turned to the lesser issue of designing a more rapid policy creation process.

While amending the current research to reflect the vulnerabilities identified in the FIST case study would assist FIST developers and reduce the risks involved in incorporating FIST into a tactical unit, as the Process modeling for the As-Is scenario demonstrated, that would be akin to "fixing today's problem's tomorrow." The current policy creation process is sluggish, particularly when compared to the rapidity of innovation surrounding smartphone technologies. This mismatch ensures that incremental corrections to existing policy will not solve the endemic lag between security policy and the edge of current technology.

Taking principles of business process reengineering, design thinking, and change management into account, this research proposed a modification to the existing policy formulation process which is more collaborative and iterative and less hierarchical or scripted. Bearing in mind the organizational and political considerations and implications of a less-controlled process, this research suggested a hybrid collaborative-hierarchical model for policy formulation based on information communications technologies which would both accelerate the process and afford sufficient top-level oversight. The results of the process improvement were discussed in the previous chapter, and are also displayed in the appendices. Suffice it to say, while the modeling in this research was entirely theoretical, the ameliorated results alone give adequate cause for excitement at the prospects of a revamped process.

The true danger to any BPR initiative lies in the reluctance to accept the radical change. For this reason, this research included quite a bit of literature concerning change management. While seemingly superfluous, the discussion of change management is in fact the lynch pin of the entire effort, since without lasting reform, the underlying mismatch between policy and smartphone technologies will remain unresolved, and the risks will only increase. It is precisely this potential for future harm which should spur

the "crisis" necessary to accept radical change. It has been the objective of this research to highlight the crisis and suggest a possible remedy.

C. SUGGESTIONS FOR FUTURE RESEARCH

During the course of this research, several opportunities for future research became readily apparent, which out of considerations for time and scope, were omitted and left for future inquirers. These possibilities are outlined below.

1. Acquisitions Process Research

As mentioned previously, the mismatch between existing policy and smartphone technologies might be solved in two ways. Given the scope of the effort in this paper, the research sought to illuminate ways in which the policy formulation process might be made more responsive and comprehensive. The alternative involves a reform of the acquisition process.

The current acquisition process is bureaucratic in the extreme, and once the process gets moving, the weight of its inertia has the potential to carry forward poor ideas and half developed concepts. Taking the business process reengineering, design thinking, and change management principles discussed in this paper, a comprehensive assessment and modeling simulation for acquisition process reforms might also bear fruit.

2. Creating Policy as a Design Thinking Exercise

This research focused on the possibilities available for correcting the systemic mismatch between policy and rapidly evolving technologies using smartphones as a case study. What this research did not do was to actually present a draft policy document developed using the proposed policy formulation process. A motivated researcher, well connected to industry and DOD stakeholders as well as to experts in the fields of information technology, computer security, and a few other creative and fertile minds, could extend this research onto its next logical step and actually produce a draft smartphone security policy document for consideration using a rapidly iterative design thinking process.

3. Creating a Secure Smartphone Using Design Thinking

Similar to the creation of a security policy using design thinking methodologies, and in keeping with Hall's (2012) research for improving the command and control systems and set up for the U.S. Navy Submarine Force, further research should consider building a secure smartphone using a design thinking process. The development of a secure mobile system in a more open and collaborative style should allow the inclusion of all of the benefits of the novel technologies while also provided for an evolutionary advantage in assessing and designing for the trade-offs in security, utility, and functionality.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. AS-IS SAVVION OUTPUT

Simulation Results		
Duration	703:15:00	Time

Process Time And Cost

Process	Scenario	Instances	Total Cost	Waiting Time (Time)	Total Time (Time)
DODIssuances	(default)	36	573632.21	7668:30:00	13126:00:00

DODIssuances

Scenario	(default)
Instances	36

Activity	Performer	Occurs	Waiting Time (Time)	Time To Complete (Time)	Total Time (Time)
Distribute	Office of the Secretary of Defense	36	0:00:00	36:00:00	36:00:00
Posting Review	Office of the Secretary of Defense	36	**0:45:00**	9:00:00	9:45:00
Signature	Office of the Secretary of Defense	36	0:00:00	36:00:00	36:00:00
Legal Objection Review	Office of the General Council	36	**25:30:00**	72:00:00	97:30:00
Legal Sufficiency Review	Office of the General Council	36	**102:30:00**	180:00:00	282:30:00
Post Issuance to Portal 3	Directives Division	36	**216:30:00**	18:00:00	234:30:00
Post Issuance to the Portal	Directives Division	36	**192:15:00**	18:00:00	210:15:00
Post issuance to the Portal	Directives Division	36	**233:30:00**	18:00:00	251:30:00
Precoordination Edit	Directives Division	36	**92:30:00**	219:45:00	312:15:00
Presignature Review	Directives Division	36	**144:15:00**	219:45:00	364:00:00
Provide Clearance	Defense Office of Prepublication and Secur	36	**2:00:00**	72:00:00	74:00:00
Assign Number to Issuance	Component	36	**468:15:00**	36:00:00	504:15:00
Comply with OGC recommen	Component	25	**323:30:00**	50:00:00	373:30:00
Determine External Coordin	Component	36	**517:00:00**	36:00:00	553:00:00
Incorporate Directives Edit	Component	36	**516:45:00**	72:00:00	588:45:00
LSR Revisions	Component	9	**74:15:00**	18:00:00	92:15:00
Obtain Signatures	Component	36	**482:45:00**	18:00:00	500:45:00
Prepare Action Memo	Component	36	**395:15:00**	36:00:00	431:15:00
Prepare Routing Form	Component	36	**538:30:00**	36:00:00	574:30:00
Prepare the Final Package	Component	36	**275:45:00**	72:00:00	347:45:00
Request DOPSR Clearance R	Component	36	**307:30:00**	18:00:00	325:30:00
Request Formal Coordinatio	Component	36	**499:00:00**	18:00:00	517:00:00
Request LOR	Component	36	**515:00:00**	18:00:00	533:00:00
Request Legal Sufficiency R	Component	36	**398:30:00**	18:00:00	416:30:00
Request Presignature Revie	Component	36	**444:30:00**	18:00:00	462:30:00
Revise the Issuance	Component	36	**423:45:00**	72:00:00	495:45:00
Write Issuance	Component	36	**464:30:00**	108:00:00	572:30:00
OSD Inbox 1	Any member of Office of the Secretary of D	36	0:00:00	351:00:00	351:00:00
OGC Inbox 1	Any member of Office of the General Coun	36	0:00:00	288:00:00	288:00:00
OGC Inbox 2	Any member of Office of the General Coun	36	0:00:00	720:00:00	720:00:00
EA Inbox 1	Any member of External Agencies Inbox	36	0:00:00	648:00:00	648:00:00
Formal Coordination	Any member of External Agencies	36	**14:00:00**	72:00:00	86:00:00
DOPSR Inbox 1	Any member of DOPSR Inbox	36	0:00:00	198:00:00	198:00:00
DD Inbox 1	Any member of Directives Division Inbox	36	0:00:00	432:00:00	432:00:00
DD Inbox 2	Any member of Directives Division Inbox	36	0:00:00	432:00:00	432:00:00
DD Inbox 3	Any member of Directives Division Inbox	36	0:00:00	342:00:00	342:00:00
DD Inbox 4	Any member of Directives Division Inbox	36	0:00:00	432:00:00	432:00:00

Resource	Unit	Cost/Unit	Threshold	Usage	Cost
Any member of External Ag	Hour	338.5	0	72	$24,372.00
Any member of DOPSR Inbo	Hour	0	0	198	$0.00
Office of the Secretary of D	Hour	520.61	0	81	$42,169.41
Any member of Office of the	Hour	0	0	351	$0.00
Office of the General Counci	Hour	404.34	0	252	$101,893.68
Component	Hour	338.5	0	644	$217,994.00
Any member of Directives D	Hour	0	0	1638	$0.00
Directives Division	Hour	331.04	0	493	$163,202.72
Any member of Office of the	Hour	0	0	1008	$0.00
Defense Office of Prepublica	Hour	331.04	0	72	$23,834.88
Any member of External Ag	Hour	0	0	648	$0.00

Performers Queue Length and Utilization

Name	Average	Min	Max	Utilized(%)	Idle(%)
Any member of External Ag	0.02	0	2	10.24	89.76
Any member of DOPSR Inbo	0	0	0	0.94	99.06
Office of the Secretary of D	0	0	1	11.52	88.48
Any member of Office of the	0	0	0	1.66	98.34
Office of the General Counci	0.18	0	4	35.83	64.17
Component	9.45	0	24	91.57	8.43
Any member of Directives D	0	0	0	7.76	92.24
Directives Division	1.25	0	10	70.17	29.83
Any member of Office of the	0	0	0	4.78	95.22
Value of 'Creator'	0	0	0	0	100
Generic	0	0	0	0	100
Defense Office of Prepublica	0	0	1	10.24	89.76
Any member of External Ag	0	0	0	3.07	96.93

Bottlenecks

Process	Activity	Performer	Avg Queue Length	Min Queue Length	Max Queue Length
DODIssuances	Assign Number to Issuance	Component	0.67	0	3
DODIssuances	Comply with OGC recommendations	Component	0.46	0	2
DODIssuances	Determine External Coordination	Component	0.74	0	3
DODIssuances	Formal Coordination	Any member of Exte	0.02	0	2
DODIssuances	Incorporate Directives Edit	Component	0.73	0	4
DODIssuances	LSR Revisions	Component	0.11	0	1
DODIssuances	Legal Objection Review	Office of the Genera	0.04	0	2
DODIssuances	Legal Sufficiency Review	Office of the Genera	0.15	0	4
DODIssuances	Obtain Signatures	Component	0.69	0	3
DODIssuances	Post Issuance to Portal 3	Directives Division	0.31	0	5
DODIssuances	Post Issuance to the Portal 2	Directives Division	0.27	0	3
DODIssuances	Post issuance to the Portal	Directives Division	0.33	0	5
DODIssuances	Posting Review	Office of the Secreta	0	0	1
DODIssuances	Precoordination Edit	Directives Division	0.13	0	2
DODIssuances	Prepare Action Memo	Component	0.56	0	3
DODIssuances	Prepare Routing Form	Component	0.77	0	3
DODIssuances	Prepare the Final Package	Component	0.39	0	2
DODIssuances	Presignature Review	Directives Division	0.21	0	3
DODIssuances	Provide Clearance	Defense Office of Pr	0	0	1
DODIssuances	Request DOPSR Clearance Review	Component	0.44	0	3
DODIssuances	Request Formal Coordination	Component	0.71	0	3
DODIssuances	Request LOR	Component	0.73	0	4
DODIssuances	Request Legal Sufficiency Review	Component	0.57	0	3
DODIssuances	Request Presignature Review	Component	0.63	0	3
DODIssuances	Revise the Issuance	Component	0.6	0	3
DODIssuances	Write Issuance	Component	0.66	0	3

Note:	Red-marked Waiting Time values indicates "Activity has waiting time"
	Red-marked Usage values indicates "Usage crossed threshold"

APPENDIX B. AS-IS KVA

	KVA - No REVENUE																	
	IT as a Minor Additive																	
	244 work days/year																	
	40 hour week																	
	8 Hour Day																	
	36 Actions per year																	
	.148 Actions per day																	
	Revenue per action	$ 10,000.00													Reduction	10.00%		
	Revenue/day	$ 1,480.00																
Performer	Processes	Actual Learning Time	Nominal Learning Time	Times Fired	#PEOPLE	%T	Total Learning Time	Total Output per day	Actual Work Time	Utilization per day	Total Input per day	Cost per day	NUM	DEN	ROK	Cost to Benefit Ratio	%NUM	%DEN
		Days	Days	per day					Days									
OSD	Distribute	1	1	0.0511909	1	80	81	4.146463	1	5%	0.051191	$ 520.61	$ 34.88	$ 26.65	131%	13%	2%	1%
	Posting Review	4	6	0.0511909	1	40	164	8.395308	0.27083	1%	0.013864	$ 520.61	$ 70.62	$ 7.22	978%	1%	5%	0%
	Signature	1	1	0.0511909	1	20	21	1.075009	1	5%	0.051191	$ 520.61	$ 9.04	$ 26.65	34%	29%	1%	1%
OGC	Legal Objection Review	30	12	0.0511909	1	10	330	16.893	2.70833	14%	0.138642	$ 404.34	$ 142.11	$ 56.06	254%	4%	10%	1%
	Legal Sufficiency Review	30	17	0.0511909	1	10	330	16.893	7.84722	40%	0.401706	$ 404.34	$ 142.11	$ 162.43	87%	11%	10%	4%
DD	Post Issuance to Portal 3	1	1	0.0511909	1	80	81	4.146463	6.51389	33%	0.333452	$ 331.04	$ 34.88	$ 110.39	32%	32%	2%	2%
	Post Issuance to the Portal 2	1	1	0.0511909	1	80	81	4.146463	5.84028	30%	0.298969	$ 331.04	$ 34.88	$ 98.97	35%	28%	2%	2%
	Post issuance to the Portal	1	1	0.0511909	1	80	81	4.146463	6.98611	36%	0.357625	$ 331.04	$ 34.88	$ 118.39	29%	34%	2%	3%
	Precoordination Edit	5	4	0.0511909	1	15	80	4.095272	8.67361	44%	0.44401	$ 331.04	$ 34.45	$ 146.99	23%	43%	2%	3%
	Presignature Review	3	2	0.0511909	1	10	33	1.6893	10.1111	52%	0.517597	$ 331.04	$ 14.21	$ 171.35	8%	121%	1%	4%
DOPSR	Provide Clearance	2	1	0.0511909	1	10	22	1.1262	2.05556	11%	0.105226	$ 331.00	$ 9.47	$ 34.83	27%	37%	1%	1%
Component	Assign Number to Issuance	1	1	0.0511909	1	90	91	4.658372	14.0069	72%	0.717028	$ 338.50	$ 39.19	$ 242.71	16%	62%	3%	5%
	Comply with OGC recommendations	4	6	0.0355492	1	10	44	1.564166	14.94	53%	0.531106	$ 338.50	$ 13.16	$ 179.78	7%	137%	1%	4%
	Determine External Coordination	5	3	0.0511909	1	10	55	2.815499	15.3611	79%	0.786349	$ 338.50	$ 23.68	$ 266.18	9%	112%	2%	6%
	Incorporate Directives Edit	4	3	0.0511909	1	20	84	4.300036	16.3542	84%	0.837185	$ 338.50	$ 36.17	$ 283.39	13%	78%	2%	6%
	LSR Revisions	7	3	0.0127977	1	10	77	0.985425	10.25	13%	0.131177	$ 338.50	$ 8.29	$ 44.40	19%	54%	1%	1%
	Obtain Signatures	3	2	0.0511909	1	50	153	7.832208	13.9097	71%	0.712051	$ 338.50	$ 65.89	$ 241.03	27%	37%	4%	5%
	Prepare Action Memo	3	2	0.0511909	1	30	93	4.760754	11.9792	61%	0.613224	$ 338.50	$ 40.05	$ 207.58	19%	52%	3%	4%
	Prepare Routing Form	2	1	0.0511909	1	30	62	3.173836	15.9583	82%	0.816921	$ 338.50	$ 26.70	$ 276.53	10%	104%	2%	6%
	Prepare the Final Package	5	2	0.0511909	1	60	305	15.61322	9.65972	49%	0.49449	$ 338.50	$ 131.34	$ 167.38	78%	13%	9%	4%
	Request DOPSR Clearance Review	2	1	0.0511909	1	70	142	7.269108	9.04167	46%	0.462851	$ 338.50	$ 61.15	$ 156.68	39%	26%	4%	3%
	Request Formal Coordination	2	1	0.0511909	1	70	142	7.269108	14.3611	74%	0.735158	$ 338.50	$ 61.15	$ 248.85	25%	41%	4%	5%
	Request LOR	3	5	0.0511909	1	70	213	10.90366	14.8056	76%	0.75791	$ 338.50	$ 91.72	$ 256.55	36%	28%	6%	6%
	Request Legal Sufficiency Review	2	1	0.0511909	1	70	142	7.269108	11.5694	59%	0.59225	$ 338.50	$ 61.15	$ 200.48	31%	33%	4%	4%
	Request Presignature Review	2	1	0.0511909	1	70	142	7.269108	12.8472	66%	0.657661	$ 338.50	$ 61.15	$ 222.62	27%	36%	4%	5%
	Revise the Issuance	5	3	0.0511909	1	10	55	2.815499	13.7708	70%	0.704941	$ 338.50	$ 23.68	$ 238.62	10%	101%	2%	5%
	Write Issuance	20	10	0.0511909	1	15	320	16.38109	15.9028	81%	0.814077	$ 338.50	$ 137.80	$ 275.57	50%	20%	9%	6%
Externals	Formal Coordination	4	8	0.0511909	1	20	84	4.300036	9.75	50%	0.499111	$ 338.50	$ 36.17	$ 168.95	21%	47%	2%	4%
	Sum	153	100				3508	176			13.6		$ 1,480.00	$ 4,637.20	32%	31%		
	Correlation	90%																

SO = Savion Output

Total Activity time (Utilization)	
OSD	11.6%
OGC	54.0%
Directorates Div	195.2%
DOPSR	10.5%
Component	1036.4%
External Agencies	49.9%

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. TO-BE SAVVION OUTPUT

Simulation Results					
Duration	522:15:00	Time			

Process Time And Cost

Process	Scenario	Instances	Total Cost	Waiting Time (Time)	Total Time (Time)
DODIssuances	As Is	72	409294.8	0:00:00	1854:00:00

DODIssuances

Scenario	As Is
Instances	72

Activity	Performer	Occurs	Waiting Time (Time)	Time To Complete (Time)	Total Time (Time)
Distribute	Office of the Secretary	72	0:00:00	18:00:00	18:00:00
Posting Review	Office of the Secretary	72	0:00:00	18:00:00	18:00:00
Signature	Office of the Secretary	72	0:00:00	72:00:00	72:00:00
Directives Editing	Directives Division	72	0:00:00	36:00:00	36:00:00
Provide Clearance	Defense Office of Prep	72	0:00:00	144:00:00	144:00:00
OSD Inbox 1	Any member of Office	72	0:00:00	360:00:00	360:00:00
Legal Inbox	Any member of Office	72	0:00:00	144:00:00	144:00:00
Final Legal Review	Any member of Office	72	0:00:00	72:00:00	72:00:00
Legal Editing	Any member of Office	72	0:00:00	36:00:00	36:00:00
Formal Coordination Editing	Any member of Extern	72	0:00:00	36:00:00	36:00:00
DOPSR Inbox 1	Any member of DOPSI	72	0:00:00	144:00:00	144:00:00
Portal Inbox	Any member of Direct	72	0:00:00	144:00:00	144:00:00
Assign Number to Issuance	Any member of Comp	72	0:00:00	18:00:00	18:00:00
Coallate Edits	Any member of Comp	72	0:00:00	144:00:00	144:00:00
Draft Issuance	Any member of Comp	72	0:00:00	144:00:00	144:00:00
LSR Revisions	Any member of Comp	18	0:00:00	36:00:00	36:00:00
Obtain Signatures	Any member of Comp	72	0:00:00	36:00:00	36:00:00
Post issuance to the Portal	Any member of Comp	72	0:00:00	36:00:00	36:00:00
Prepare Action Memo	Any member of Comp	72	0:00:00	72:00:00	72:00:00
Prepare the Final Package	Any member of Comp	72	0:00:00	144:00:00	144:00:00
Request DOPSR Clearance R	Any member of Comp	72	0:00:00	36:00:00	36:00:00
Request Legal Sufficiency R	Any member of Comp	72	0:00:00	36:00:00	36:00:00

Resource	Unit	Cost/Unit	Threshold	Usage	Cost
Any member of DOPSR Inbo	Hour	0	0	144	$0.00
Office of the Secretary of D	Hour	520.61	0	108	$56,225.88
Any member of Office of the	Hour	0	0	360	$0.00
Any member of Office of the	Hour	404.34	0	108	$43,668.72
Any member of Component	Hour	338.5	0	702	$237,627.00
Any member of Directives D	Hour	0	0	144	$0.00
Directives Division	Hour	331.04	0	36	$11,917.44
Any member of Office of the	Hour	0	0	144	$0.00
Defense Office of Prepublica	Hour	331.04	0	144	$47,669.76
Any member of External Ag	Hour	338.5	0	36	$12,186.00

Performers Queue Length and Utilization

Name	Average	Min	Max	Utilized(%)	Idle(%)
Any member of DOPSR Inbo	0	0	0	27.57	72.43
Value of 'Creator'	0	0	0	0	100
Generic	0	0	0	0	100
Office of the Secretary of D	0	0	0	20.68	79.32
Any member of Office of the	0	0	0	68.93	31.07
Any member of Office of the	0	0	0	6.89	93.11
Any member of Component	0	0	0	33.6	66.4
Any member of Directives D	0	0	0	27.57	72.43
Directives Division	0	0	0	6.89	93.11
Any member of Office of the	0	0	0	27.57	72.43
Defense Office of Prepublica	0	0	0	27.57	72.43
Any member of External Ag	0	0	0	0	100
Any member of External Ag	0	0	0	6.89	93.11

Bottlenecks

Process	Activity	Performer	Avg Queue Length	Min Queue Length	Max Queue Length

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D. TO-BE KVA

KVA - No REVENUE
IT as a Minor Additive
244 work days/year
40 hour week
8 Hour Day
72 Actions per year
.148 Actions per day
Revenue per action $ 10,000.00
Revenue/day $ 1,480.00

Reduction 10.00%

Performer	Processes	Actual Learning Time Days	Nominal Learning Time	Times Fired per day	#PEOPLE	%T	Total Learning Time	Total Output per day	Actual Work Time Days	Utilization per day	Total Input per day	Cost per day	NUM	DEN	ROK	Cost to Benefit Ratio	%NUM	%DEN
OSD	Distribute	1	3	0.137865	1	80	81	11.16707	0.25	3%	0.034466	$ 520.61	$ 62.46	$ 17.94	348%	35%	4%	2%
	Posting Review	4	8	0.137865	1	40	164	22.60986	0.25	3%	0.034466	$ 520.61	$ 126.47	$ 17.94	705%	1%	9%	2%
	Signature	1	3	0.137865	1	20	21	2.895165	1	14%	0.137865	$ 520.61	$ 16.19	$ 71.77	23%	44%	1%	6%
DD	Directives Editing	3	4	0.137865	1	10	33	4.549545	0.5	7%	0.068933	$ 331.04	$ 25.45	$ 22.62	112%	9%	2%	2%
DOPSR	Provide Clearance	2	4	0.137865	1	10	22	3.03303	2	28%	0.27573	$ 331.04	$ 16.96	$ 91.28	19%	54%	1%	8%
OGC	Final Legal Review	30	14	0.045955	3	10	330	45.49545	5	23%	0.689325	$ 404.34	$ 254.47	$ 278.72	91%	11%	17%	24%
	Legal Editing	30	18	0.045955	3	10	330	45.49545	2	9%	0.27573	$ 404.34	$ 254.47	$ 111.49	228%	4%	17%	10%
Externals	Formal Coordination Editing	1	3	0.137865	1	80	81	11.16707	1	14%	0.137865	$ 338.50	$ 62.46	$ 46.67	134%	7%	4%	4%
Component	Assign Number to Issuance	1	7	0.0344663	4	90	91	12.54572	0.5	2%	0.068933	$ 338.50	$ 70.17	$ 23.33	301%	3%	5%	2%
	Coallate Edits	3	4	0.0344663	4	20	63	8.685495	0.5	2%	0.068933	$ 338.50	$ 48.58	$ 23.33	208%	5%	3%	2%
	Draft Issuance	2	4	0.0344663	4	10	22	3.03303	2	7%	0.27573	$ 338.50	$ 16.96	$ 93.33	18%	55%	1%	8%
	LSR Revisions	1	4	0.0086166	4	20	21	0.723791	2	2%	0.068933	$ 338.50	$ 4.05	$ 23.33	17%	58%	0%	2%
	Obtain Signatures	2	4	0.0344663	4	20	42	5.79033	0.25	1%	0.034466	$ 338.50	$ 32.39	$ 11.67	278%	4%	2%	1%
	Post issuance to the Portal	1	3	0.0344663	4	90	91	12.54572	2	7%	0.27573	$ 338.50	$ 70.17	$ 93.33	75%	13%	5%	8%
	Prepare Action Memo	4	4	0.0344663	4	20	84	11.58066	2	7%	0.27573	$ 338.50	$ 64.78	$ 93.33	69%	14%	4%	8%
	Prepare the Final Package	3	5	0.0344663	4	70	213	29.36525	2	7%	0.27573	$ 338.50	$ 164.25	$ 93.33	176%	6%	11%	8%
	Request DOPSR Clearance Review	3	4	0.0344663	4	50	153	21.09335	0.5	2%	0.068933	$ 338.50	$ 117.98	$ 23.33	506%	2%	8%	2%
	Request Legal Sufficiency Review	3	4	0.0344663	4	30	93	12.82145	0.5	2%	0.068933	$ 338.50	$ 71.72	$ 23.33	307%	3%	5%	2%
	Sum	95	100				1935	265			3.1		$ 1,480.00	$ 1,160.31	128%	8%		
	Correlation	94%																

SO = Savion Output

Total Activity time (Utilization)	
OSD	20.7%
OGC	32.2%
Directorates Div	6.9%
DOPSR	27.6%
Component	37.1%
External Agencies	13.8%

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX E. FRAMEWORK FOR POLICY PROCESS CHANGE

The following chapter provides the theoretical framework for the approach to analysis and change regarding policy and the policy formulation process through a discussion of the interrelated fields of Business Process Reengineering (BPR), Knowledge Value Added (KVA), Change Management, and Design Thinking.

D. BUSINESS PROCESS REENGINEERING

1. Background of Process Improvement Techniques

When Hammer and Campy (1993) popularized the term "business process reengineering," they touted the end of the industrial age and heralded the rise of a new, postindustrial era. Hammer and Campy (1993) contended that as a result of that shift, into what we might now call the age of design, a topic which will be covered later in this paper, many of the cornerstones industrial age practice have become irrelevant in today's business environment. Adam Smith (1956) classified the paradigm of the industrial age as the division of labor and economies of scale in his 1776 *The Wealth of Nations*, and it was on these assumptions that industrial era corporations were built and organized. Fundamentally, these corporations broke complex processes into numerous highly simplified and specialized tasks that even poorly educated workers could perform efficiently (Brewster, 1997). Smith showed how by dividing the process of making straight pins into 18 tasks, each of which was coordinated and integrated by layers of management, 10 employees could increase their productivity from less than 100 pins a day to 48,000. The management echelons and functions in turn served as the foundation of the modern bureaucracy (Smith, 1956). In keeping with the concept of division of labor and economies of scale, the separation of the production process encouraged similar division in management of organizations into simplified and separated manageable management tasks (Hammer & Champy, 1993).

Despite the historical success of industrial age practices, Hammer and Champy (1993) concluded that that very same set of management principles in fact hinder modern organizations' ability to compete in this, the post-industrial age, and viewed

reengineering as the method of change to realize new ways of doing business. In response to the simple question, "If the industrial era paradigm worked for over 200 years why change now?", Brewster (1997) posited that just as in the private sector, where global competition has placed increased demands on businesses for effectiveness and efficiency with which industrial age techniques cannot cope, so too in the public and government sectors the pressure of public and congressional scrutiny mandates a change in process.

2. Process Improvement Strategies

As there are many differing perspectives on how one might approach problem solving, so too are there multiple flavors of process improvement (Brewster, 1997). Harrington (1991) ascribed to the need to continuously improve current processes in order to enjoy gains in efficiency and effectiveness. On the other end of the spectrum, Hammer and Champy (1993) proposed that radical changes which attained breakthrough order-of-magnitude improvements are necessary to sustain an organization over the long term.

This research identified three conceptual strategies for process improvement whose differences lie primarily in their theoretical approach and the prescribed rate of change. These three strategies for process improvement are: continuous process improvement (CPI), business process redesign, and business process reengineering (BPR).

a. Continuous Process Improvement

Continuous process improvement (CPI), which stems from the overarching concept of total quality management (TQM), aims to discover and correct problems occurring in the current process. Employees and Self-managed teams are encouraged and empowered to make task-level improvements in quality, cycle-time, and cost at the lowest level (Brewster, 1997). While CPI is typically performed within a particular business function, it may also involve cross-functional teams to a limited extent. The goal of implementing CPI is to have it become a philosophy and way of life within the organization. Thus, in its ideal CPI is continuous, and employees are constantly finding

problems, identifying the causes, and incrementally modifying the process to fix those problems (Brewster, 1997).

In the CPI strategy, performance gains are modest, and incremental (usually between 5-10 percent improvements in cost, time, or customer satisfaction). CPI also carries with it comforting advantages in terms of costs and risk. CPI incurs low costs as the level of organizational change and level of effort required to detect, correct, and adapt to the changes is low. CPI also mitigates risks as the investment cost for the change effort and the total scope of the change is again modest and incremental. (Davis 1994, Caudle 1995). Regarding information technology tools to assist with CPI, there are a number of well-defined tools available for use that require a only a moderate degree of training and learning time (e.g., control charts, Pareto diagrams, flow charts, cause and effect diagrams, histograms) (Brewster, 1997).

b. Business Process Redesign

As Brewster (1997) described, Business Process Redesign entails streamlining processes by eliminating activities which do not add positive value as well as efforts to integrate tasks in a process. Furthermore, in in process redesign strategy, direction setting and strategic planning from the corporate level focus cross-functional teams on specific improvement objectives (rather than simply letting the groups find their own issues). The overall feel and flow of the existing processes generally remains intact, and accompanies moderate increases in performance, and little to moderate changes in organizational structures (Davis 1994, Caudle 1995, Brewster, 1997). Finally, risk to process improvement success is increased as compared to CPI due to the increased levels of organizational change required (e.g., culture, tasks, structure, and roles) (Brewster, 1997).

c. Business Process Reengineering

What separates BPR from the previous two strategies is that the philosophical approach to BPR hinges on the radical redesign of a process to dramatically increase performance. To that end, BPR focuses on delving to the root of things, and beyond merely fixing what is already in place, BPR seeks to discern fundamentally novel means of performing work (Hammer & Champy, 1993). The philosophy of BPR rejects the

notion that significant performance and efficiency gains may be achieved through incremental improvements alone (Brewster, 1997). Hammer and Champy (1993) define BPR as

> The fundamental rethinking and radical redesign of business processes to achieve dramatic improvements in critical, contemporary measures of performance, such as cost, quality, service and speed. (Hammer and Champy, 1993, p .32)

Put simply, BPR entails starting fresh and rebuilding a process from the ground up (Davis 1994, Hammer 1993). In BPR cross-functional teams, which may also include non-organizational members such as customers, consultants, and facilitators, tear apart and then completely redesign a process end-to-end. As the scope of this change is the entire process, implementing BPR successfully almost always requires a high degree of organizational change both in an entity's technical infrastructure and potentially even culture (Brewster, 1997). To achieve such results in the face of organizational resistance, BPR efforts are top-down projects which leverage leadership and strategic planning. Another key aspect of BPR is that, as opposed to CPI, BPR employs information technology to reengineer new processes rather than reinforcing existing processes (Brewster, 1997).

Figure 17 compares and contrasts critical features of each of the aforementioned process improvement strategies:

Features	Continuous Process Improvement	Business Process Redesign	Business Process Reengineering
Philosophy	Improve what you do in functional or sub-activity; Accepts status quo — current processes are what customers need	Accepts current process; Remove "hand off" activities of little value in an end-to-end examination	Focus on critical broken processes; Alter or replace basic approach to doing business in jobs, skills, structures, systems, culture
Timing	Part of a way of life to continuously improve; project results in short time frames	Done on a periodic basis; improvement may take a few months for simple efforts; 1 to 2 years if efforts are more complex	Used selectively; sub-process deployment may take several months; full deployment across an entire complex process may take 2 to 5 years
Scope	Little emphasis on interrelationship of business processes in a business system; internal focus	Coverage of many sub-processes and "turf"; internal focus	Scope is entire process or major sub-processes that cover broad cross-functional areas; includes interfacing outside the organization
Leadership	Broad-based, bottom-up	Both bottom-up and top-down, more senior leadership needed	Management focused, top-down; significant senior management attention and time
Means	Generally, improvement work done by work unit part-time teams; use of quality tools	Improvement work often done by diversified task forces or teams that cross functions	Improvement generally done by dedicated teams representing end-to-end activities; work facilitated by process sponsors and owners
Performance Gains	Incremental: Slightly increases (5-10%) performance	Moderately increases performance	Revolutionary: Greatly increases performance
Costs, Risks, Pain	Low: Resources generally easily handled within existing budgets and personnel allocations; small iterative investments; low-level effort offers few risks; pain of implementation is minimal	Low to moderate: Resources may require shifting funds and personnel or adding more funds and personnel; risks increase somewhat as more activities are involved, implementation pain covers more activities	High: Resources require significant funding and dedicated personnel allocations; large, upfront investments; risks greatly increase given extensive process coverage; implementation pain is high

Figure 17. Process Improvement Approaches (from Caudle, 1995)

Thorough examination of Figure 17 leads one to conclude that while all are oriented on a process customer focus. At the macro level the distinctions between the improvement strategies lie primarily as matters of scope and levels of organizational change required for successful implementation (Brewster, 1997). In this regard, it is also possible to view the process improvement strategies on a continuum from the minimally invasive CPI at one end, to the massively destructive and radical BPR on the opposite end as shown in Figure 18.

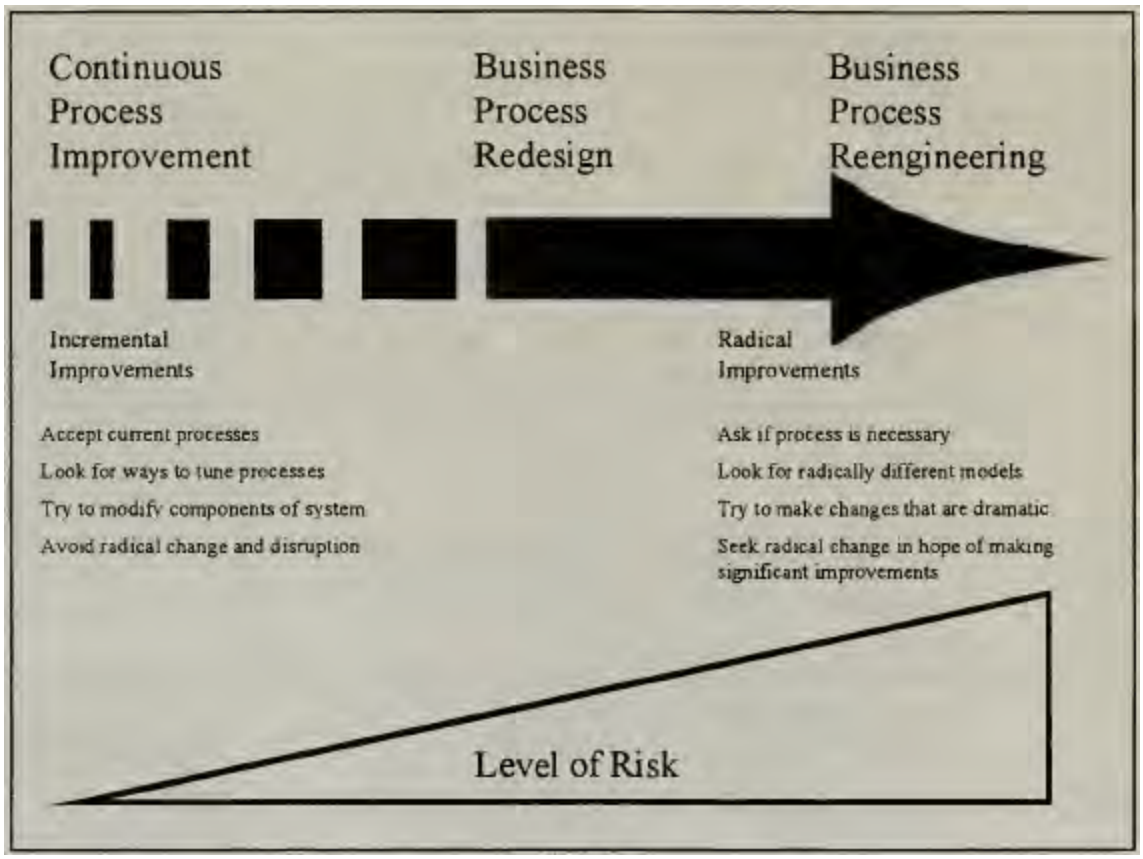

Figure 18. The Process Improvement Continuum (from Brewster, 1997)

Integrating BPR into an organization which practices Lean and Six Sigma is best done from a strategic vision/top level leadership standpoint. BPR is considered top-down and revolutionary in that it should produce radical results that dramatically alter an organization, particularly in an effort to avoid or mitigate significant pain. Lean and Six Sigma on the other hand are more focused on eliminating waste and reducing variation, respectively, and are the more contemporary terms used to describe the CPI strategy mentioned above. As such, Lean and Six Sigma advocate continuous incremental improvement of processes from the bottom up. Therefore, while a company which does Lean/Six Sigma is likely to have a good understanding of its processes, BPR and Lean/Six Sigma are in a sense at odds with each other in that the latter seek to improve upon the status quo whereas the former seeks to destroy and rebuild it. As O'Neill and Sohal (1999) asserted. however, the combination of the two conceptual business process improvement frameworks provides for a total improvement package as incremental

improvements from Lean/Six Sigma are good in the short term, and BPR is good over the long term. Thus, major BPR efforts (which cannot be sustained indefinitely) should still be followed by TQM/CPI/Lean/Six Sigma efforts to produce maximum process improvements as shown in Figure 19.

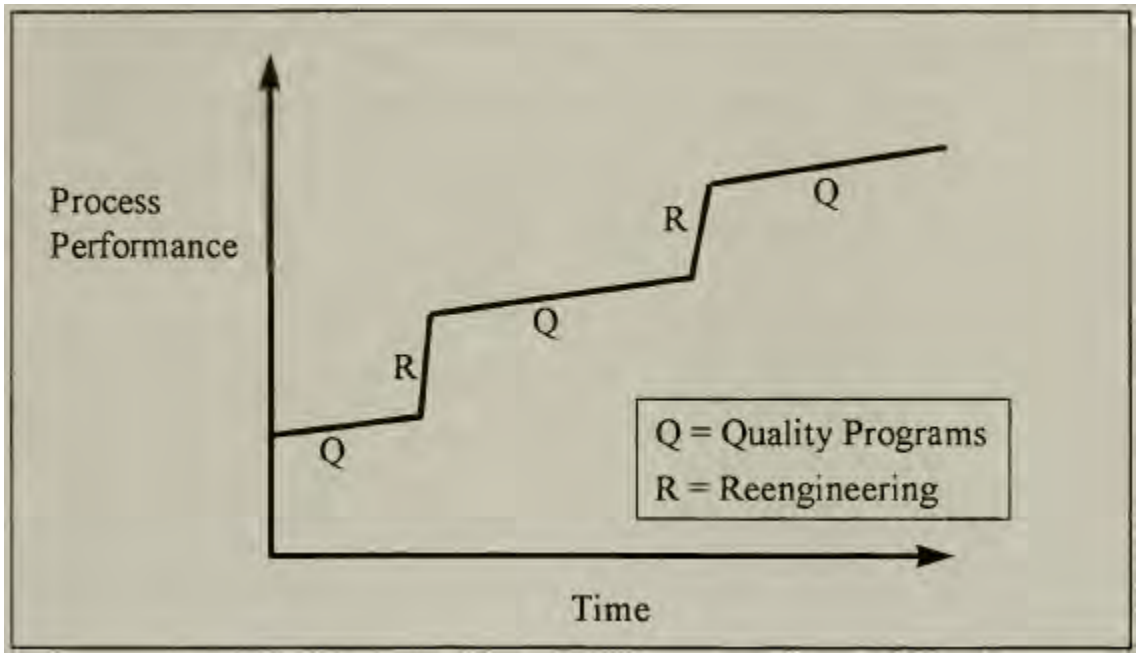

Figure 19. Combination of BPR and CPI (from Brewster, 1997)

3. Business Process Reengineering for the DOD

While there is no simple formula for reengineering any organization, certain constraints for the DOD make the process increasingly complex. Reengineering within the DOD occurs in a political milieu, where a starting from scratch methodology is typically impractical (Brewster, 1995). More specifically, the number and outlook of the various stakeholders for any DOD process are myriad. Bryson (1995) defined stakeholders as "any person, group, or organization that can place a claim on an organization's attention, resources, or output or is affected by that output." For the DOD, such stakeholders could include legislative and executive authorities and interests, the taxpayers, the media, special interest groups, unions, and a host of internal and external agencies that provide resources for, or receive services from, the DOD, not to mentioned

international partners and allies. The true complexity of BPR within the DOD becomes evident when one considers that these stakeholders influence political support, are party to or drivers of policy determinations, and exercise near total authority over funding (Caudle, 1995). Caudle further defined the notion of reengineering in government:

> Government business process reengineering is a radical improvement approach that critically examines, rethinks, and redesigns mission-delivery processes and sub processes. In a political environment, it achieves dramatic mission performance gain from multiple customer and stakeholder perspectives. It is a key part of a process management approach that continually evaluates, adjusts, or removes processes or sub process for optimal performance. (Caudle, 1995, pp. 10)

Thus, BPR within government, while it may follow the same theoretical methodology as BPR in any other context, that is, radical redesign and revolutionary change, the ability to achieve success requires additional consideration of the increased number of stakeholders and their degrees of control.

4. Conclusion

From the discussion of BPR and TQM above, and in light of the fundamental mismatch between the user requirements to rapidly evolving technology and the policy process which governs accessibility, a radical redesign of the policy formulation process is in order. Naturally, it follows that incremental, that is CPI, strategies might ease the pain, but not sufficiently to correct the underlying issue. In this sense, editing the current policy to encompass and address the latest developments can be viewed as a short-term, continuous improvement. The objective of this research is to discuss how a redesign might happen, and what it might look like. While BPR provides a conceptual framework for the type of change needed, an examination of three subsequent fields of study is required to complete the foundation. Those fields are Knowledge Value Added, Change Management, and Design.

E. KNOWLEDGE VALUE ADDED

In very general terms, the Industrial Age sought to turn people, via an assembly line process, into automatons specially trained for a specific task and organized optimally

(hierarchically) to perform it ceaselessly. In the modern Information Age, computers have allowed us to automate machines, and in effect reverse the shackling of human beings to the mundane repetitive tasks required under the old paradigm. To that end, the real value of human beings is in their execution of knowledge in performing a task. Thus, as Stewart (1997) postulated,

> Knowledge has become the preeminent economic resource—more important than raw material; more important, often, than money. Considered as an economic output, information and knowledge are more important than automobiles, oil, steel, or any of the products of the Industrial Age.

Knowledge value added (KVA) theory, then, is squarely rooted in the Information Age, and analyzes the performance of knowledge within an organization's core processes in terms of the returns that knowledge generates (Housel & Bell, 2001, p. 93). While KVA is derived from a sophisticated breakdown of thermodynamics, it is in fact straightforward to apply, and can be applied to nearly any level of any organization (Housel & Bell, 2001, pp. 91–93). The fundamental assumptions of KVA are outlined in Figure 20.

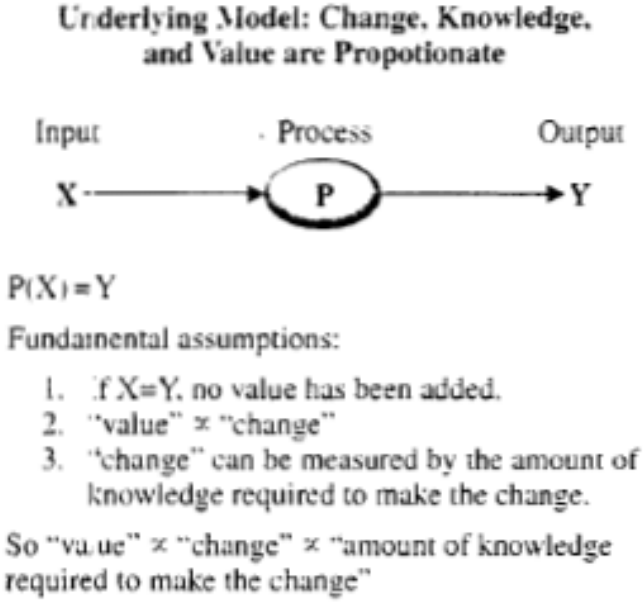

Figure 20. Fundamental Assumptions of KVA (from Housel &Bell, 2001, p. 94)

1. Knowledge

By extrapolation, several other axioms of KVA become apparent as well. Indeed, as Housel and Bell (2001, p. 94) asserted, these assumptions are valid whether the knowledge executed is in people's heads, or in an IT system, which also implies that the knowledge can be explicit, or tacit. KVA derives common units of knowledge as observed in the execution of core processes and relates them to terms of price and cost. Thus the end result of a KVA analysis is a set of ratios which compare the price and cost of the knowledge units (Housel & Bell, 2001, p. 94). To adequately capture the knowledge in a process, the KVA methodology turns to measuring the learning time incurred to gain proficient use of the knowledge.

2. Learning Time

As the measurable component of knowledge, the learning time is represented as the process (read time) to gain use of knowledge (Housel & Bell, 2001). For example, if I can be shown how to write a cursive letter in one minute, but it takes me three hours of continuous practice to be able to master writing one on my own, then my learning time for that activity is three hours. While the example is quotidian in that we would not add the time it took a person to master writing every letter into the learning time required to write a collegiate-level essay, it serves to illustrate the point that tasks require time to master; time which is separate from the time it takes to instruct someone in the performance of the task. It is the time required to master use that KVA seeks to capture.

As with knowledge, use of the learning time construct carries with it similar axioms. Namely, learning can also be explicit or tacit, and learning time is related to a specific activity. In this sense, logically, learning time is related directly to the complexity of the task (Housel & Bell, 2001). It is also key to note that learning time as a measure in KVA analysis is concerned with the learning time in use, not the learning time residing in 'inventory.' In other words, a person might have a tremendous amount of skills in a variety of fields, but for KVA the only learning measured is the learning time required for the particular task involved in the core process being evaluated. Put more simply, while the learning time to become a neurosurgeon is no doubt extreme, the

totality of that learning time (which would certainly be many years) cannot be used as a measure of the only task the surgeon performs in a process is to verify a prescription was written accurately (which might only in truth have taken a learning time of hours to days). Thus, as alluded to in the previous discussion of knowledge as an economic resource, knowledge, and by extension learning time, are the 'machines' that drive output and revenue (Housel & Bell, 2001).

As mentioned before, the knowledge, and hence the learning time, could reside within a person, or within information technology (IT). As such, the learning time in a process represents the summation of the human and IT learning times (Housel & Bell, 2001, p. 98). Moreover, learning time can be measured ordinally, nominally, or in terms of actual learning time, and generally two different sets of subject matter experts will each come up with the learning time in a process or sub-process using a different method such that the two can be compared to provide transparency and accuracy.

3. KVA Methodology

Conducting a KVA analysis begins, as with any other corporate change or analysis technique, with identifying the core areas or processes to evaluate. The evaluators would then gather data on the amount of knowledge in each sub-process by using the learning time approach. Then, a sufficient sampling time would be measured to capture a representative sample of the processes final output. In order to view the amount of knowledge executed in the process, the total learning time would then be multiplied by the number of times the process was executed in the sample period. With the total amount of knowledge executed in hand, revenue and costs may be allocated to each component of the sub-process. It is the addition of revenue (often based on market comparables) with costs that provides the ratios necessary to obtain return on knowledge (ROK) results for interpretation (Housel & Bell, 2001, p. 98). Figure 21 illustrates the KVA methodology in terms of measuring learning time, process description, and a binary query method.

Steps	Learning time	Process description	Binary query method
1.	Identify core process and its subprocesses.		
2.	Establish common units to measure learning time.	Describe the products in terms of the instructions required to reproduce them and select unit of process description.	Create a set of binary yes/no questions such that all possible outputs are represented as a sequence of yes/no answers.
3.	Calculate learning time to execute each subprocess.	Calculate number of process instructions pertaining to each subprocess.	Calculate length of sequence of yes/no answers for each subprocess.
4.	Designate sampling time period long enough to capture a representative sample of the core process's final product/service output.		
5.	Multiply the learning time for each subprocess by the number of times the subprocess executes during sample period.	Multiply the number of process instructions used to describe each subprocess by the number of times the subprocess executes during sample period.	Multiply the length of the yes/no string for each subprocess by the number of times this subprocess executes during sample period.
6.	Allocate revenue to subprocesses in proportion to the quantities generated by step 5 and calculate costs for each subprocess.		
7.	Calculate ROK, and interpret the results.		

Figure 21. Three Approaches to KVA (from Housel and Bell, 2001, p. 95)

4. Implications of KVA

Of the many implications the use of KVA analysis portends for organizations is the argument for moving knowledge which resides inside human employees into IT. As Housel and Bell (2001) attested, organizations should move knowledge into IT systems when that knowledge is simple, procedural knowledge that fires frequently, or when the knowledge is volatile knowledge that might be lost when employees leave the organization.

Take the first argument. Is it necessary for people to become specially trained to format documents, or prepare routing forms? Rather, can this knowledge be transferred into an IT system which automatically performs the task? In this case, submitting a report involves both human and IT components, since the human still had to master the type of skill necessary to generate the report's contents, and the IT system performed the formatting and routing. This arrangement capitalizes on the creative potential of the human mind without shackling it to mundane, repetitive processes which a machine can accomplish ceaselessly and flawlessly.

As for the second argument, retraining personnel is costly and time consuming. Worse, if only one person knows how to execute a process since that is the only position devoted to it, and that person is likely to leave or move on frequently, it makes sense to capture the knowledge in an IT system rather than risk losing it every time there is personnel turnover. While many organizations have attempted to capture such knowledge using binders full of standard operating procedures, desktop procedures, and turnover materials, at the fundamental level the new employee must still learn the procedure nonetheless (recall the discussion of the difference between learning time and instruction time). Hence, if possible, it makes more sense to transfer the knowledge to an IT system and not risk its loss.

While KVA provides an organization with insight into how it makes use of its intellectual capital, as well as areas to target for improvement, KVA methodology does not discuss how to go about making these changes. To tackle that aspect, the discussion turns now to the fields of Change Management and Design.

F. CHANGE MANAGEMENT AND DESIGN THINKING

1. Change Management

Put succinctly, change management is a field of study aimed at improving the rate of successful implementation of changes within an organization. The change management field is vast, includes many notable works, and provides numerous frameworks for thinking about and planning organizational change (Hall, 2012). Given the more restricted scope of this research, this section will provide only a broad outline of change management theory with the goal of elucidating how difficult even a small modification can be in a hierarchical process within a large organization such as the DOD. This research drew heavily on Hall's (2012) discussion of change management in his thesis regarding the Tactical Advancements for the Next Generation (TANG) Forum, as well as referenced John P. Kotter's works: 1996's *Leading Change* and 2002's *The Heart of Change*, David Gleicher's change formula as modified by Dannemiller and Jacobs in their 1992 article, *Changing the Way Organizations Change*, and Professor Peter Senge's *The Fifth Discipline*.

a. Creating Change

The revised change formula Dannemiller and Jacobs (1992) advanced is

$$D \times V \times F > R$$

In this formula D represents dissatisfaction with the status quo, V represents the proposed and idealized vision of the future, F represents the first steps taken toward the vision, and R is the amount of resistance to be overcome. These values are all relative, and not absolute, and objective measurement for each is possible. Even a cursory mathematical examination of this formula implies that if a change effort is to succeed, the product of the dissatisfaction, the vision and the first steps toward the vision must be greater than the total amount of resistance applied against the change (Hall, 2012). It is also readily apparent that if any of the three factors working to create the change (dissatisfaction, vision, and first steps) is absent, then that side of the equation is reduced to zero, and the resistance is insurmountably greater (Dannemiller & Jacobs, 1992). More importantly, as Hall (2012) attested, while this formula does not guarantee the change effort will be successful, a firm grasp of the basic underlying concepts and theory is a prerequisite for fruitful discussion and problem framing for introducing and sustaining organizational change.

While Kotter (2002, Kindle, location 87)) rightly posited that change management is a discussion or analysis of people's behavior, Hall (2012) asserted that

> The dissatisfaction and the vision are things provided by management or leadership to the members of the organization. The first steps are a plan drawn up by management for the organization's members to follow, and personnel, likely at all levels of the organization, generate the resistance. (p. 12).

This researcher agrees with Kotter's assertion, yet believes Hall's is overly simplistic, and representative of an idealized hierarchical model wherein leadership is well-attuned to organizational problems and brilliant in seeing the future. It is certainly valid to think leadership *might* be dissatisfied, as well as that leadership must be involved in any vision for the future. However, this discussion ignores the very real possibility that the people at the very lowest levels of the organization are dissatisfied with some aspect of the organization, have their own vision of how things should be, and indeed,

take some steps toward realizing that vision. In that scenario, it may well be the leadership which provides the resistance to change.

In his *Heart of Change*, Kotter (2002) further refines his statement that change hinges on people's behavior by noting that the action which induces true change is "speaking to people's feelings." Kotter (2002, Kindle location 112, 125) proffered the opinion that a reasoned analysis aimed at impacting people's thoughts is significantly less likely to alter their behavior than if they are "shown a truth that influences their feelings." This is an important point and bears additional explanation. It becomes apparent that while it may be possible to convince someone with facts that some form of change is in his or her best interests, that realization alone is unlikely to create the behavioral change required to achieve the vision. The type of enduring and meaningful change necessary necessitates an emotional connection to the change and reasons behind it (Hall, 2012). In concluding that line of thought, Kotter (2002, Kindle location 129) stated definitively, "The flow of see-feel-change is more powerful than that of analysis-think-change." Jonathan Haidt (2012, Kindle page 47) rephrased the same notion in his work, *The Righteous Mind: Why Good People are Divided by Politics and Religion*, when he attested "You can't make a dog happy by forcibly wagging its tail. And you can't change people's minds by utterly refuting their arguments." This discussion is in the context of this research as it underscores the simple yet critical point that pure factual argument alone (and to an extent a drawn out research paper) is unlikely to succeed in getting people to adopt new modes of behavior *even when they cognitively understand why they should*.

Kotter (2002, Kindle location 403) expands upon the discussion of change management in providing organizational leadership with an "eight-stage change process." Through the course of detailed discussions with corporate leadership, he discovered that while the stages may overlap, is it important they be kept in sequence in order for the cumulative effect of building upon one another toward realizing the change to occur (Hall, 2012). The first four stages revolve around preparing the organization to reorient itself. The next three stages entail the introduction of the new direction, and the final stage is where the newly implemented change is made and integrated into the culture and

practice of the organization so that the change might be an enduring one (Kotter, 2002, Kindle location 376).

The eight stages of Kotter's (2002, Kindle location 375) change process are:

- Establishing a Sense of Urgency
- Creating the Guiding Coalition
- Developing a Vision and Strategy
- Communicating the Change Vision
- Empowering Broad-Based Action
- Generating Short-Term Wins
- Consolidating Gains and Producing More Change
- Anchoring New Approaches in the Culture

Interestingly, though not surprisingly, the eight stages can be mapped fairly readily to Gleicher's change formula. Stage one corresponds to the dissatisfaction with the status quo; stages two through four correspond with the proposed future vision of the organization; and stages five, six and seven represent the first steps toward achieving the change (Hall, 2012).

(1) Establishing a Sense of Urgency

The reason establishing a sense of urgency is so critical is that if the individuals within the organization feel that everything is going just fine, they will never embrace a change. Thus the sense of urgency serves to loosen the grip of complacency upon the organization (Hall, 2012). As the change formula suggests, it is the sense of dissatisfaction with the status quo that creates the willingness to be open to a new vision (Hall, 2012).

(2) Creating the Guiding Coalition

Good leaders in the both the civilian sector and within the military must develop a central core group of supporters for their change efforts (Hall, 2012). A change vision may not yet exist, but this core group should be comprised of adventurous "early adopters" that are motivated to improve the organization and dedicated to spreading the new vision (Moore, 1991, Kindle Location 297).

(3) Developing a Vision and Strategy

It is incumbent on the leader, in partnership with the guiding coalition to create and present a clear and simple vision statement which paints the picture of the future of the organization (Hall, 2012). As Kotter (1995, Kindle Location 183) attested, the purpose of the vision is to "direct, align, and inspire actions on the part of large numbers of people." The simplicity and clarity of the vision cannot be overstated. Kotter's (1995, Kindle Location 202) rule for corporate visions was, "whenever you cannot describe the vision driving a change initiative in five minutes or less and get a reaction that signifies both understanding and interest, you are in for trouble."

(4) Communicating the Change Vision

As noted previously, one of the reasons for creating a guiding coalition is that communicating the vision is of the utmost importance. As Hall (2012) stated, "the vision creates its maximum effect when all members of the organization have a common knowledge and understanding of it and embrace it." Unfortunately, it is fairly common that organizational leadership fails to communicate the vision they have created for the company effectively (Kotter, 1995, Kindle Location 1400). It is insufficient to present the vision once or twice, and then assume that the entire population of the organization understands, and more importantly, embraces, the new direction. This is particularly salient given the fact that the average employee is bombarded with many other competing inputs and requirements (Hall, 2012). Kotter (1995, Kindle Location 1442) also highlighted a second and equally critical component of communicating the vision is "leadership by example." Indeed, the surest method for undermining the vision is for leadership (the very people who espouse the new direction), to behave in a manner inconsistent with the message being communicated (Hall, 2012).

(5) Empowering Employees for Broad-Based Action

Kotter (1995, Kindle Location 1548) defined this stage as the removal of four types of "barriers to empowerment" for an organization's employees. The first barriers are structural, and entail determining if the structure of the organization prevents effective employee actions as they work to embrace the change. The second set of barriers focus on employee skills, and revolve around whether or not employees have

been provided the appropriate skill sets and training required to make the change (Kotter, 1995, Kindle Location 1610). The third set of barriers are those of the underlying organizational system. These barriers hinge on whether or not legacy organizational processes have been amended to reflect the new direction (Hall, 2012). The final barrier is almost counterintuitive as it stems from whether the supervisors themselves are a barrier to the adoption of the change. Indeed, while top-level leadership may well be on board, subordinate leaders might still act counter to the new vision, thereby ruining the impression of the entire leadership structure's support (Hall, 2012).

(6) Generating Short-Term Wins

Though the long term prize should be kept visible, the members of the organization need to experience small victories which convince them that the ultimate change effort will be successful. Kotter (1995, Kindle Location 1772) referred to the need for short-term wins as "managing the current reality." As Kotter (1995, Kindle Location 1817) outlined, a worthwhile short-term win is visible, unambiguous, and related to the change effort underway. Short-term wins maintain the change's momentum, and build credibility for the vision in the eyes of those who remain uncommitted or even resistant (Hall, 2012).

(7) Consolidating Gains and Producing More Change

Ensuring the change effort progresses until the final desired end-state is attained requires constant pressure since resistance to the change effort never dissipates completely (Hall, 2012). While counterintuitive, celebrating a short-term win can send the message that no further effort is required, and induce a regression toward legacy processes and beliefs (Kotter, 1995, Kindle Location 1983). It is key to note that the pain, or perceived upcoming future pain, which the sense of urgency created is uncomfortable, and hence the organization changes as a result of this discomfort. Thus victories, no matter how small, give the impression that the pain should let up. After all, isn't that the cause for the celebration? It becomes readily apparent that despite the short-term win, constant pressure will be required to maintain the sense of urgency in spite of the achievements along the way.

(8) Anchoring New Approaches in the Culture

This final stage is in essence a continuation of the aforementioned stage, but goes beyond mere achievement of the desired result. This stage is focused on cementing the change into the organization's culture such that the results become self-sustaining (Kotter, 1995, Kindle Location 2197). In other words, if this stage is accomplished successfully, and the state change has been internalized, the departure of one individual, even if it is the visionary leader himself, should not derail the change.

b. Resistance to Change

As Hall (2012) posited, and as indicated by the change formula, a constant pressure toward maintaining the status quo works against the effort placed into the changing. For the change effort to succeed, this resistance must be overcome. Kotter (1995, Kindle Location 1996) stated that while there are naturally some forces which resist the initial change implementation effort, there are other, separate forces which seek to subvert the effort throughout its life cycle. In *Heart of Change,* Kotter described four types of behavior that tend to derail the initial change effort:

> the first is complacency, driven by false pride or arrogance. A second is immobilization, self-protection, a sort of hiding in the closet, driven by fear or panic. Another is you-can't-make-me-move deviance, driven by anger. The last is a very pessimistic attitude that leads to constant hesitation. (Kotter, 2002, Kindle Location 338)

Moving to the second set of resistance factors, Kotter then provided eight reasons for resistance to change throughout a change effort's life cycle. These factors, which can be found in *Leading Change* (Kotter, 1995, Kindle Location 362), are:

- Inwardly Focused Cultures
- Paralyzing Bureaucracy
- Parochial Politics
- Low Levels of Trust
- Lack of Teamwork
- Arrogant Attitudes
- Lack of Leadership in Middle Management
- The General Human Fear of the Unknown

The final aspect of an organization's resistance to change is that of system dynamics. While the struggle between the innovators and early adopters against the laggards may be divisive and protracted, neither side is to blame for this contentiousness: he entire organization works as a system. As Senge (1990, p. 67) pointed out, there is no "separate other;" all of the protagonists and antagonists are part of a single system. The cure, therefore, lies in one's relationship with the "enemy."

c. Conclusion

Change management, while an invaluable resource to leverage when implementing organizational change, does not in and of itself guarantee success. Change management only improves the odds of a successful effort (Hall, 2012). The change management field also fails to outline how to create a vision, and does not identify the steps necessary to implement that vision in a practical sense. In order to delve into practical concerns regarding how one might adapt a highly bureaucratic process such as DOD policy-making, a journey into a separate but related field is required to strip away the final level of abstraction from the heretofore esoteric and academic discussion. That field is design.

2. Design Thinking

Since there are a multitude of conceptions and misconceptions surrounding design and design thinking, this paper will refer to the idea of "design thinking" by making use of Brown's (2009) original description from *Change by Design*: "Design thinking relies on our ability to be intuitive, to recognize patterns, to construct ideas that have emotional meaning as well as functionality, to express ourselves in media other than words or symbols." The mention of emotional meaning in addition to functional meaning is perhaps the critical aspect of design thinking. This theme will resurface later on in the discussion of applying design thinking to problem solving. Another interesting aspect of design thinking is that in incorporating the emotional component of problem solving, good design solutions not only solve the problems for which they were developed, but also others which were not anticipated (Boland & Collopy, 2004, Kindle Location 264).

The rapidly iterative process of design thinking sets it apart from standard "linear problem-solving (Liedtka & Ogilvie, 2011, Kindle Location 230)." Liedtka and Ogilvie (2011, Kindle Location 230) portray the linear problem-solving processes as problem definition, solution identification and analysis, followed by the selection of the "correct" choice. On the other hand, design solutions are based primarily upon empathy and experimentation (Liedtka & Ogilvie, 2011, Kindle Page 230). The stark contrast between the two methodologies is clear, and one may surmise that adherence to one over the other might reflect not only a penchant for a particular process, but even a separate world view.

Senge (1990, Kindle Page 321) underlined the importance of design thinking to an organization in his view that organizational leaders neglect the role of a "leader as designer" in terms of how view themselves. In this context, Senge's argument for the role of the leader as designer suggests that the leader should focus on constructing the organization to maximize interaction between the organization's members rather than be the primary driver of new ideas (Hall, 2012). Therefore, the leader is concerned with how his organization thinks, not what it thinks. Design thinking, therefore, is a conceptual problem solving framework for tackling any problem, internal or external, an organization may face (Hall, 2012). As Senge (1990, Kindle Location 207) attested,

> It's just not possible any longer to figure it out from the top, and have everyone else following the orders of the "grand strategist." The organizations that will truly excel in the future will be the organizations that discover how to tap people's commitment and capacity to learn at all levels in an organization.

To help guide the leader, Liedtka and Ogilvie (2011, Kindle Location 377-399) presented three basic growth lessons derived from observation of those who implemented design thinking into their organizations successfully. These growth lessons are:

- You don't have to search far and wide to find opportunities. There are opportunities to improve through design in everything we do and what we surround ourselves with.
- You don't have to bet big in order to be successful. In fact, big bets often cause failure. Place small bets fast, and learn, learn, learn.
- Speed thrills. Developing a corporate climate that thinks, moves and innovates fast can become addictive and lead to continuous improvements and learning.

Liedtka and Ogilvie (2011, Kindle Location 4414-438) also provided several maxims for growth. Hall (2012) explained that several of these maxims hold high relevance for the DOD. As such, the relevant growth maxims for the DOD are "Focus on meeting genuine needs" and "Explore multiple options." The first maxim stresses the need for empathy concerning the customer for which the product, process or organization is being designed (Hall, 2012). The second maxim touches back on the idea of placing small bets quickly in order to learn from experience. In other words, this highlights the idea of rapid and simultaneous prototyping of several options at once. Of particular note, this method is not equivalent to the prototyping the DOD performs through its acquisitions process for major systems. Rather, the design thinking version of prototyping emphasizes the use of "inexpensive materials to examine the problem as opposed to building a couple of multi-million dollar weapon systems to compete against one another and be analyzed for failure modes" (Hall, 2012).

a. Innovation

Senge (1990, Kindle Page 5) describes an innovation in simple terms as an invention that can be dependably reproduced at a practical cost. From this definition, one can extrapolate that while design thinking will therefore probably generate innovation, an innovation or innovative process may or may not incorporate elements of design thinking.

From the literature on innovation, design, and design thinking, it is commonly accepted that most mature and established organizations optimize and specialize themselves over time for the efficient performance of routine activities (Govindarajan & Trimble, 2010, Kindle Location 347, 356). This organizational occurrence does not indicate fault in the company, but rather stems from the natural tendency to maximize the cost to benefit ratio, particularly as it applies to processes which are predictable and routine. However, Govindarajan and Trimble (2010, Kindle Location 358) also contended that such specialization bring two distinct aspects of the organization into conflict; namely what they referred to as the "performance engine" and the innovators. These two forces represent what James March (1991) termed the "exploitation" and

"exploration," elements of an organization, respectively. Described concisely, the performance engine, or exploitation, portion of the organization is focused on ensuring daily operations remain efficient and profitable, while the innovators, or exploration, portion seeks to find new products or processes.

As resources within any organization are always somewhat scarce, both Govindarajan and Trimble (2010) and March (1991) portrayed the two segments as in conflict and competition. The typical business is generally not well organized or disposed to balance the two, and as such, maintaining a healthy equilibrium and relationship between them must to some degree fall to leadership and management (Hall, 2012).

b. Empathy

As noted previously, empathy is at the heart of design thinking. Liedtka and Ogilvie (2011, Kindle Location 194) argued that, "Design starts with empathy, establishing a deep understanding of those we are designing for." Tim Brown (2009), CEO and President of IDEO, described the presence of empathy as the distinguishing characteristic between design thinking and purely academic exercises. In his words,

> We are not trying to generate new knowledge, test a theory, or validate a scientific hypothesis—that's the work of our university colleagues and an indispensable part of our shared intellectual landscape. The mission of design thinking is to translate observations into insights and insights into products and services that will improve lives. (Brown, 2009, Kindle Location 627)

In *Wired to Care*, Patnaik and Mortensen (2009), described empathy as "seeing the world as it really is." This definition seems somewhat rosy, so perhaps trying to see reality from someone else's frame of reference and trying to understand how they experience their reality is a better means of describing empathy (Hall, 2012). Regardless, seeing reality through the eyes of the customer for whom the output of the design process is intended is nevertheless a relevant and critical goal.

c. The Design Process

As there are many different versions and examples of design processes, this paper will rely primarily on that outlines in the *Bootcamp Bootleg* from Stanford University's Hasso Platford Institute of Design, also known as the d. school.

The Bootcamp Bootleg lists five phases of their design process. They start with "empathize," and move through "define," "ideate," and "prototype" to conclude with testing. Works on Design by Brown (2009) and Cross (2011) also allude to the existence of a precursory design phase: The Brief.

The Brief. Before the designers can launch into an empathic investigation of the problem space, Hall (2012) explained that the designers typically receive a brief consisting of the goals and constraints for the project. While the goals often seem straightforward, they frequently require further examination, and may change over time. This evolution stems from the fact that while customers bring set design goals to the effort initially, these goals must generally be adapted to a higher level of abstraction in order to apply the design process (Hall, 2012). As an example, the customer might open the design effort with the goal to "improve aluminum can recycling on Wednesdays." Elevating this goal to make it more applicable to a design process, the goal might become might become, "How do we increase awareness of recycling opportunities? (Hall, 2012)" Stanford's d.school and Tim Brown (2009, Kindle Page 194) described such questions as "How might we" questions or "HMWs."

From the simple discussion above, it becomes relatively clear that the brief is necessary to orient the designers to the problem space, but that it is hardly set and in stone and will tend to evolve as the designers further define the problem. The brief should bound the problem space and provide direction to the designers, but should not be overly restrictive such as to eliminate the type of creative problem solving inherent in the design process. Indeed, Cross (2011, Kindle Location 256) presented his thoughts on what the brief should be by highlighting that the reason for a degree of flexibility in the brief is to allow the designers to define and refine the problem as they attempt to solve it. Furthermore, and of significance, Cross did not hold the brief to represent a concrete set

of requirements or specifications for the final product. To reinforce the point, Cross highlighted a statement from his interview with architect Richard MacCormac about design wherein MacCormac asserted that "often in competitions the winning scheme is the one that tells the client something that they never knew before … something that is terribly important to them and was not in the brief (Cross, 2009, Kindle Location 256)."

Empathize. The empathize phase, also known as the observation phase, revolves around focusing the designer's empathy toward the actual user for the product or process (Kelley, 2001, Kindle Page 25). Empathizing with the end user can be difficult, particularly as the customer, i.e. the one paying for the design effort, is typically not the actual consumer of the product or process (Hall, 2012).

Senge (1990, Kindle page 63) offered a pithy description of the criticality of the "empathize" phase, and noted the high likelihood that best insight garnered from the research will be something small, and something heretofore unnoticeable. As he proffered, "Small changes can produce big results –but the areas of highest leverage are often the least obvious (Senge, 1990, Kindle page 63)." Senge (1990, Kindle page 63) furthered his analysis by orienting the empathy phase into a systems thinking approach, and attested that the most obvious methods for creating the desired impact are perhaps the least likely to create the desired effect, while "small, well-focused actions can sometimes produce significant, enduring improvements, if they're in the right place." Therefore, the underlying goal of the empathize phase is to find leverage points, or in other words, "to find the points at which maximum effort may be applied optimally to produce the greatest effect for the customer's user experience" (Hall, 2012).

Define. IDEO referred to the define stage as "generating insights" (Hall, 2012). Once the information, feelings and emotions are gathered, the define phase begins. As Hall (2012) suggested, "Seldom can the user describe what is missing or required to perform their job in the form of a complete solution. It is typically necessary to synthesize the inputs of the users into a couple of insights." It is these insights which are then used to guide the "point of view" perspective of the design sessions, focus the design effort on the needs of the user, as well as be the source of the "How might we" questions used in the brainstorming portion of the next phase (Hasso Plattner).

Ideate. This phase has been alternatively referred to as brainstorming as the goal is to create a substantive pool of ideas from which to later choose (Brown, 2009, Kindle location 852). As two-time Nobel Prize winning chemist Linus Pauling posited, "To have a good idea, you must first have lots of ideas (Brown, 2009, Kindle location 855)." Kelley (2001, Kindle location 738) outlined that brainstorming is the "the idea engine of IDEO's culture," and the aforementioned HMWs focus brainstorming sessions around the problem space and the end user. To stimulate people's creative potential, and to fully embrace Pauling's theme, IDEO follows seven self-explanatory rules in its "ideating" sessions:

- Defer Judgment
- Encourage Wild Ideas
- Build on the Ideas of Others
- Stay Focused on Topic
- One Conversation at a Time
- Be Visual
- Go for Quantity (Hasso Plattner)

In addition to the rules for ideation listed above, Brown (2009, p. 81) and Cross (2011, Kindle location 216) also suggest sketching as an invaluable practice to reinforce and elucidate ideas during brainstorming. Cross (2011, Kindle location 216) noted brainstorming sketches served as a "temporary, external store for tentative ideas" to assist the designer in presenting his idea where words alone might be insufficient. Kelley (2001, Kindle location 734) also recommended that brainstorming sessions be limited to sixty minutes in duration, due to the substantial levels of mental exertion entailed.

From the rules and suggestions above, it becomes obvious that brainstorming is guided yet unscripted process. This is not to say that "anything goes." On the contrary, brainstorming is a focused and taxing process oriented on the rapid generation of ideas from which to choose, and more importantly, the interchange between different people and their ideas. Kelley (2001, Kindle location 848-868) listed a set of procedures which are sure to stifle and stymie any true brainstorming session.

His list of “Six Ways to Kill a Brainstormer” are:

- The Boss Gets To Speak First
- Everybody Gets A Turn
- Experts Only Please
- Do It Off-Site
- No Silly Stuff
- Write Down Everything

The initial objective of the brainstorming session, as mentioned, is the generation of a large pool of ideas from which to choose. Once this large pool exists, and better yet, if the ideas are all sketched out in some visual form, the ideas are grouped, or further divided into sub-groups depending on the number, by function or other criteria (Hasso, Plattner). Once grouped, the design team selects the most popular ideas through voting or other means of consensus (Hasso Plattner).

Prototyping. As the Bootcamp Bootleg described, the objective in the prototyping phase is to translate the most popular ideas selected from the ideation phase down from the conceptual level of abstraction and into a physical setting. Kelley (2001, Kindle location 1456) outlined that prototyping is not only more engaging than mere sketches, but also creates an environment conducive to envisioning the potential solution and how that solution might be adapted to better meet the needs of the brief.

While prototyping is a well understood means for reducing risk prior to going into full production, which consequently is why the DOD also requires prototypes as part of its project management process, the prototyping described in this design process differs markedly (Bolland & Collopy, 2004, Kindle location 3541-3542). As Hall (2012) commented, the principle difference between the two is that the prototyping phase of the design process is done early on the development cycle, and is also “done in order to engage the imagination through tactile interaction with a very low cost, low risk form of possible solutions.” At a relatively low cost, the project is thereby defined through experimentation early on in the process. As Boehm and Basili’s (2001) research showed, significant investment in the requirements analysis and design phases of software development portends the possibility to reduce the cost of subsequent error correction by

a factor of 100. Boland and Collopy (2004, Kindle location 3541-3542) highlighted that the physical manifestation and manipulation of ideas allows the designers to provide feedback on potential solutions from an experiential rather than conceptual basis.

As intimated above, "these early prototypes are intended to be created and evaluated quickly and cheaply" in order to gain the insights from physical interaction without creating an emotional "overinvestment" between the designer and the prototype (Hall, 2012). Brown (2009, Kindle location 1148) noted that a rapid build and discard or move forward methodology through the use of low-cost materials early in the development process minimizes the risks associated with proceeding upon a poor idea, and increases the chances of discovering new opportunities. Moreover, such rapid and inexpensive prototyping is not limited to design of a physical object, and is equally applicable to software. For instance, one could easily prototype and demonstrate software interfaces using Post-it notes instead of having to write multiple iterations of code (Brown, 2009, Kindle location 1173).

Testing. Testing provides the design team with the opportunity to observe the end user interacting with the prototype and receive feedback (Hasso Plattner). Naturally, the phases of the design thinking process are continuous throughout, and as such there exists the "opportunity to brainstorm about how to conduct the test itself, and then prototype the test if desired" (Hall, 2012). Since most of the excitement in design thinking revolves around the brainstorming and prototyping phases, the testing phase is also less substantively detailed in the literature (Hall, 2012).

d. Failure

As Hall (2012) explained, one of the aspects which sets design thinking apart is its tolerance for, and even encouragement of, failure. Indeed, this notion is borne out in one of IDEO's core philosophies: "fail early to succeed sooner (Brown, 2009, Kindle location 228)." Other literature also stresses the iterative growth which accompanies failure. In *Yes to the Mess*, Professor Barrett (2012, Kindle location 887) remarked that accepting failure can often lead one along "the pathway to discovery, especially in highly experimental and innovative cultures." It is important to note that in this context failure

is not catastrophic cancellation of a major DOD acquisitions system, but rather the rapid generation and reformulation of the problem space and potential solutions. Thus these early failures are those of requirements analysis and solution design which serve as a cost effective and swift means of experimentation (Hall, 2012). From this discussion, it becomes plain to see that such "failures" should be encouraged and allowed to happen as early into the process as possible in order to avoid costly rework later on in the process.

e. Morale

Two other significant aspects of design thinking and the design thinking process become evident in any reading of the subject area, and relate to the morale of designers and participants (Hall, 2012). First, the literature suggests that the very process of empathy-building engenders a degree of fun and enjoyment in the workplace (Patnaik & Mortensen, 2009, Kindle location 2790). Second, and in similar fashion, Kelley (2001, Kindle location 1214) proffered a subtle but seemingly obvious idea that "When people feel special, they'll perform beyond your wildest dreams." These two concepts are not merely part of a "feel-good" speech during a relaxing yoga session. In design thinking they go to the very heart of the process; people matter. Surely the end-user is important, but so too are the designers themselves as the very productivity on which the project's success hinges is inextricably linked to the designers who go through the process.

f. Conclusion

As mentioned in the preceding paragraph, the heart of design thinking is people. The notions of creating empathy to better understand the end-user, ideation, acceptance of failure, and morale all revolve around the human being's centrality to the process. In the view of this researcher, there is potential to leverage design thinking in the DOD policy formulation process, particularly as it applies to areas of rapid technological advancement, such as smartphones, since the ideation and iterative process may well afford a more rapid means of stimulating development while at the same time allowing for comprehensive security safeguards.

G. CONCLUSION

To summarize the major components of the literature review in the context of this research, the preceding chapter discussed technological capabilities of smartphones, the higher headquarters policies which encourage the use of smartphones, and a conceptual discussion of business process reengineering, change management, and design thinking. The following chapters will provide particulars about the FIST system, specifically issues which have arisen in its implementation and use, and examine the extent of the mismatch between current policies and the policy creation process and existing technologies.

APPENDIX F. SAVVION PROCESS MODELER

A complete description of how to use Savvion's process modeler can be found in *Gear up! Savvion Process Modeler…in 20 Minutes or Less*, Savvion's program tutorial (Savvion, 2006). For the sake of brevity, the basics of how Savvion takes inputs and translates them into outputs will be discussed here.

The process modeler allows even non-technical stakeholders to intuitively and graphically depict and analyze a business process. This is done primarily through three components: performers, swim lanes, and activities. A performer is an actor or entity (such as a group of actors) which executes a function inside the business process. The first thing one does in creating a Savvion model is to create performers, as shown in Figure 22, who take the actions therein:

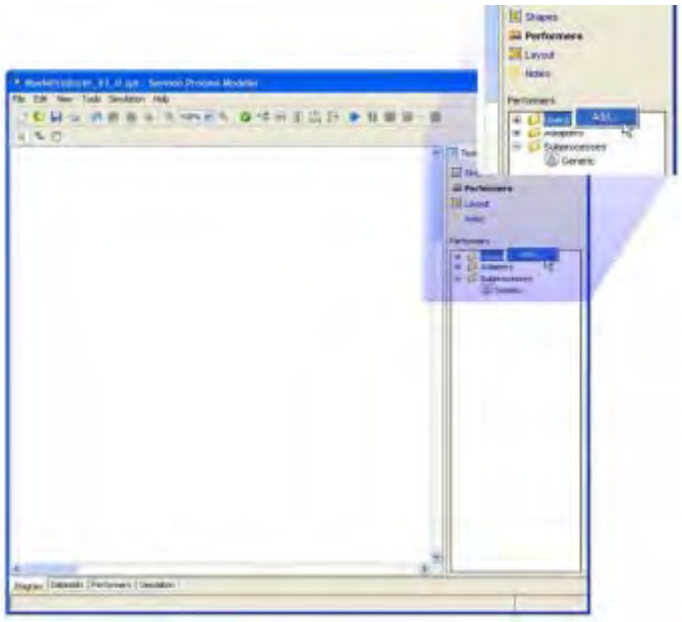

Figure 22. Dialogue Box for creating a Performer (from Savvion, 2006, p. 9)

Additional aspects of a performer are the type of performer (single actors or a group), as well as the group size, group rate, and whether all members of the group must perform an action, or if any single member may perform it (in this sense consider that any mechanic of the many in an auto body shop can perform work on a car, but *all* members

of a jury must be present during a hear or when reaching a verdict). It is in these boxes that the pay rates presented in chapter 4 were entered. Figure 23 displays how to enter settings for a performer's attributes.

Figure 23. Performer Attributes (from, Savvion, 2006, p. 10)

Once the performers are set up, the process modeler prompts a user to create swim lanes. Per the tutorial,

> Used in workflow diagrams to organize processes across functional boundaries, Swim Lanes are horizontal sections that delineate which performer is responsible for a group of task steps. A benefit of Swim Lanes is that when an Activity task step is dragged to a Swim Lane (or

moved from one Swim Lane to another), the task automatically inherits the Performer assigned to the Swim Lane. (Savvion, 2006, p. 11)

Finally, the modeler prompts the user to add activities and then links, which connect activities together within and between swim lanes. Activities are assigned to one or multiple performers and are assigned work times. As depicted in Figure 24 illustrates, links can be modified to allow for decision points, probabilities (such as the likelihood that something will have to be resubmitted, etc.).

Figure 24. Link Properties (from Savvion, 2006, p. 19)

Once the performers, swim lanes, activities, and links are created, the model is now ready to be run in a simulation. As an example, a complete Savvion process model might appear as in Figure 25.

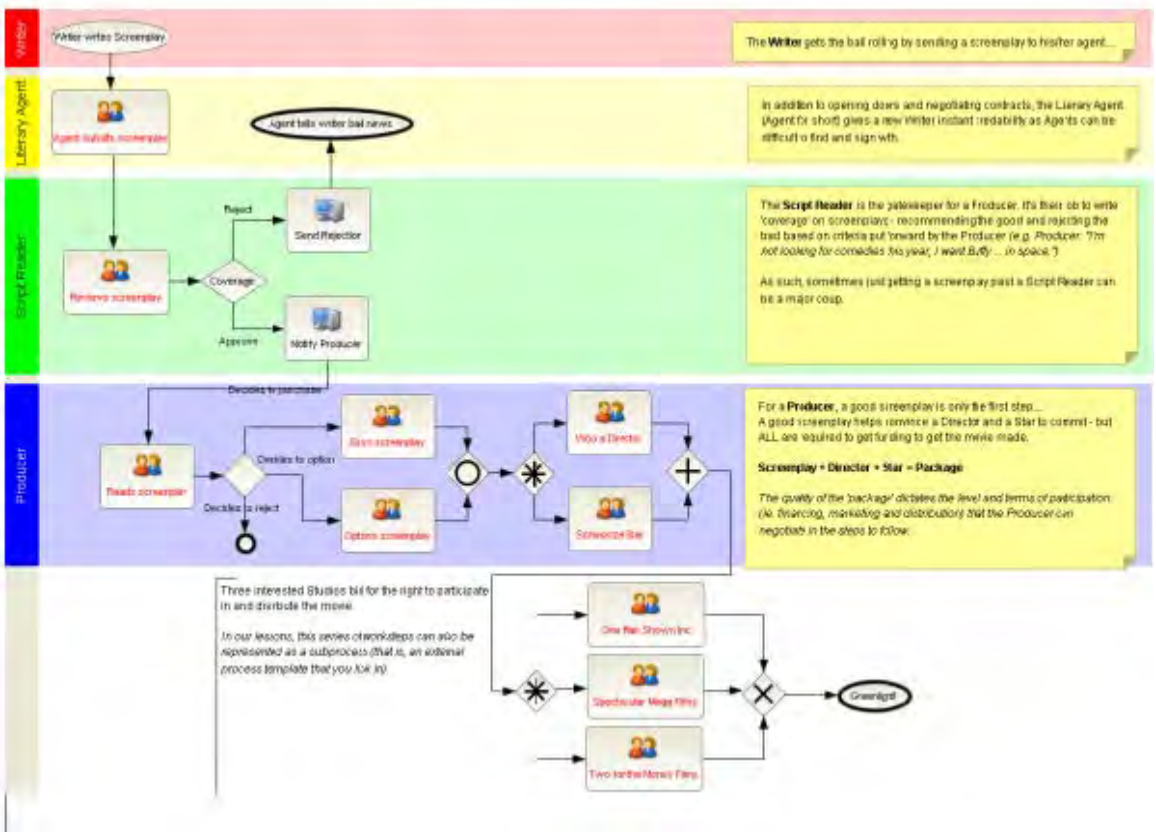

Figure 25. Complete Savvion process model (from Savvion, 2006, p. 32)

To model the process, the key elements to set are the number of instances and the interval with which they appear (in other words, how frequently the system must deal with a new instance). As discussed in chapter four, this research used one year's worth of instances in the As-Is model, and two years' worth (set to occur within a one year time span by increasing the interval) in the To-Be model. Setting the simulation is shown in Figure 26.

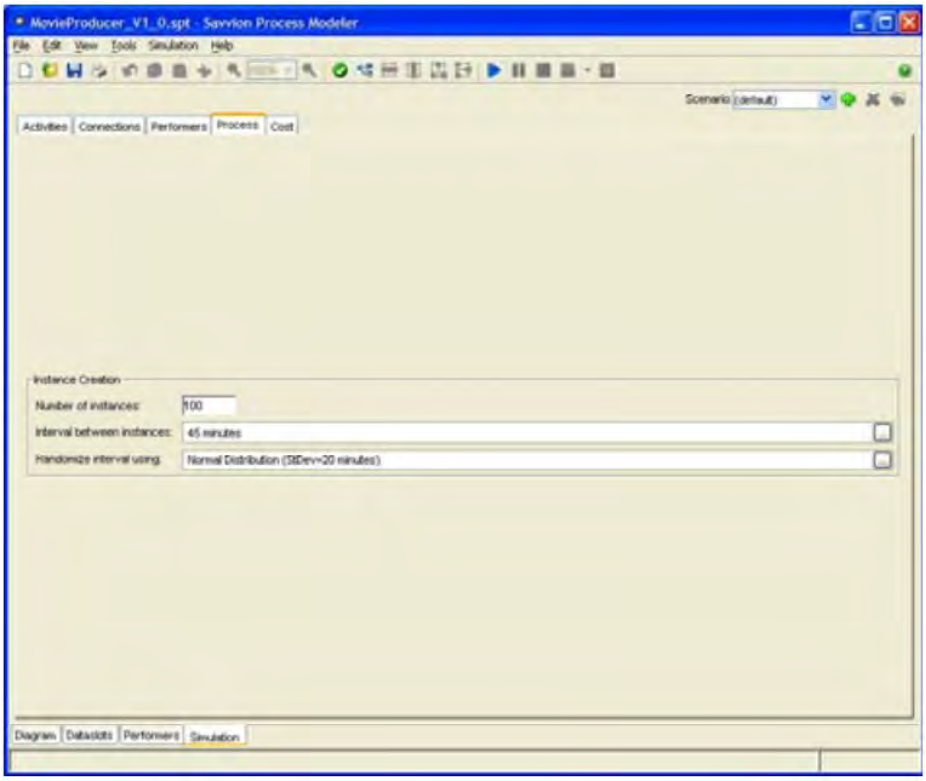

Figure 26. Savvion simulation set up (from Savvion, 2006, p. 28)

Savvion then runs the simulation, substituting a few seconds of time for each "hour" simulated (it was for this reason that this research converted work days to work hours, as mentioned in chapter four). The results come out of the model as viewed in Appendices A and C. These results break out time to complete each activity in a given swim lane, adds up the total work time required for each performer to accomplish all assigned activities, as well as depicts the time spent idle for each activity and in total. Idleness is generally a function of a bottle neck in that if a faster moving performer precedes a slower one in the process, which is in turn preceded by a regular or fast moving performer, the two more rapid performers sit around waiting for work while the slower one has a large pile sitting in its queue. Using the factors of total work time and idleness, Savvion then provides utilization percentages, essentially a measure of work efficiency, for each performer. Since hourly rates were input for each performer, this output also allows for a visualization of cost per action and total cost for the number of instances sent through the system.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Ahmed, M., & Ahamad, M. (2012). Protecting health information on mobile devices. *Proceedings of the Second ACM Conference on Data and Application Security and Privacy* (pp. 229–240). New York: ACM.

Bacon, L. M. (2011). Intel for the individual: Smartphones offer soldiers potential for specific ISR in the field. *Army Times, 71*(26), 14.

Barrett, F. J. (2012). *Yes to the mess: Surprising leadership lessons from jazz*. Boston: Harvard Business Review Press.

Boehm, B. & Basili, V. R. (2001, January). Software defect reduction top 10 list, *Software Management:* 135–137.

Boland, R. J. Jr. & Collopy, F. (2004). *Managing as designing.* Stanford: Stanford University Press.

Brewster, R. D. (1997). Business process reengineering: A primer for the Marine Corps' process owner (Master's thesis). Retrieved from http://hdl.handle.net/10945/8042

Brown, T. (2009). *Change by design: How design thinking transforms organizations and inspires innovation*. New York: Harper Collins.

Bryson, J. M. (1995). *Strategic planning for public and non-profit organizations: A guide to strengthening and sustaining organizational achievement*. San Francisco: Jossey-Bass.

Caudle, S. L. (1995). *Reengineering for results*. Washington, DC: National Academy of Public Administration Foundation.

Cha, A. E. & Nakashima, E. (2010, January 14). Google China cyberattack part of vast espionage campaign, experts say. *Washington Post*. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html?sid=ST2010011300360

Chan, W. K. (2012). Operational effectiveness of smartphones and apps for humanitarian aid and disaster relief operations: A systems engineering study (Master's Thesis). Retrieved from http://handle.dtic.mil/100.2/ADA567498

Cox, M. (2013, February 28). DOD's new mobile device plan looks to get more phones, tablets to troops. Retrieved from Defense Tech website: http://defensetech.org/2013/02/28/dods-new-mobile-device-plan-looks-to-get-more-phones-tablets-to-troops/

Cross, N. (2011). *Design thinking*. New York: Berg.

Dannemiller, K. D. & Jacobs, R. W. (1992). Changing the way organizations change: A revolution of common sense. *Journal of Applied Behavioral Science, 28*(4), 480-498.

Davis, R. J. (1994). *Framework for managing process improvement. A guide to enterprise integration*, Arlington, VA: Systems Research and Applications (SRA) Corporation/DOD (C3I).

Command, Control, Communications, and Computers (C4). (2013, April). *Marine Corps commercial mobile device strategy*. Washington, DC: C4. Retrieved from http://fedne.ws/uploads/2014_APR_USMC_mobile_device_strategy.pdf

Eaton, K. (2010). Never mind Facebook, smartphones ripe for privacy violations. Fast Company. Retrieved from http://www.fastcompany.com/1658963/smartphone-security-personal-data-lock-crime-thieves-gadgets-information-pin

Grim, N. (2013). Marine Corps mobile device strategy looks to cut costs. Defense Systems. Retrieved from http://defensesystems.com/Articles/2013/07/26/Marine-Corps-mobile-device-strategy.aspx?Page=1

Grindle, C. E. (2011). 21st century senior leader education: Ubiquitous open access learning environment (Master's Thesis). Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a543398.pdf\

Govindarajan, V. & Trimble, C. (2010). *The other side of innovation: Solving the execution challenge.* Boston: Harvard Business School Publishing.

Haidt, J. (2012). *The righteous mind: Why good people are divided by politics and religion*. New York: Pantheon Books.

Hall, T. J. (2012). A case study of innovation and change in the U.S. Navy submarine fleet (Master's Thesis). Retrieved from http://hdl.handle.net/10945/27840

Hammer, M. (1993). *Beyond reengineering: How the 21st century corporation will change our work and our lives*. New York: Harper Business.

Hammer, M. & Champy, J. (1993). *Reengineering the corporation*. New York: Harper Business.

Hasso Plattner Institute of Design at Stanford. Bootcamp bootleg. The d.school. Retrieved from http://dschool.stanford.edu/wpcontent/uploads/2011/03/BootcampBootleg2010v2SLIM.pdf (accessed February 27, 2014).

Heininger, C. (2011). Army develops smartphone framework, applications for battlefield operations. *Army Communicator, 36*(2), 56–57.

Hibbard, L. G. (2011). Communicating with the net generation. Carlisle Barracks, PA: Army War College. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a543101.pdf

Honegger, B. (2013). Student-developed smart phone app maps the "human terrain". Monterey, CA: Naval Postgraduate School. Retrieved from http://www.nps.edu/About/News/Student-Developed-Smart-Phone-App-Maps-the-Human-Terrain.html

Housel, T. & Bell, A. H. (2001). *Measuring and managing knowledge*. New York: McGraw Hill/Irwin.

Intelligence Community. (2008). Directive 503. Information Technology Systems Security Risk Management, Certification, and Accreditation. Retrieved from http://www.fas.org/irp/dni/icd/icd-503.pdf

IS&GS Defense. (n.d.). Lockheed Martin MONAX system. *MARFORPAC Background and Product Description Document* [White Paper]. Philadelphia: Lockheed Martin.

Joint Chiefs of Staff. (2013). General Martin E. Dempsey. Retrieved from http://www.jcs.mil/biography.aspx?ID=135

Kelley, T. (2001). *The art of innovation: Lessons in creativity from IDEO, America's leading design firm*. New York: Random House Digital, 2001.

Kenyon, H. (2011). Army makes strides in smart-phone security. Defense Systems. Retrieved from http://defensesystems.com/Articles/2011/01/24/Cyber-Defense-Army-Smartphone-Deployment.aspx?Page=1 (accessed March 15, 2013).

Kotter, J. P. (1995). *Leading change: Why transformation efforts fail.* Boston,: Harvard Business School Press.

Kotter, J. P. (2002). *The heart of change: Real-Life stories of how people change their organizations*. Boston: Harvard Business School Press.

Landman, M. (2010). Managing smart phone security risks. *2010 Information Security Curriculum Development Conference* (pp. 145–155). New York: ACM.

Liedtka, J., & Ogilvie, T. (2011). *Designing for growth.* New York: Columbia University Press.

Liguori, M., & Daniel, Z. (2013). Secure mobile cellular capabilities: Value analysis for expeditionary combat unit (Master's Thesis).

Longley, C. (2010). Field information support tool (Master's Thesis). Retrieved from http://calhoun.nps.edu/public/bitstream/handle/10945/5193/10Sep_Longley.pdf?sequence=1

March, J. G. (1991). Exploration and exploitation in organizational learning. *Organizational Science,(2)*1: 71–87.

Marine Corps Combat Development Command. (2013). MAGTF C2 roadmap. Arlington,VA: Headquarters Marine Corps. Retrieved from: https://www.mccdc.usmc.mil/Reference/Files/FY%202013%20MAGTF%20C2%20Roadmap.pdf

Moore, G. A. (1991). *Crossing the chasm: Marketing and selling high-tech products to mainstream customers*. New York: HarperCollins.

National Institute of Standards and Technology. (2001). Federal information processing standards publication 140-2: Security requirements for cryptographic modules. Washington, DC: U.S. Government Printing Office. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a389360.pdf

Naval Postgraduate School Public Affairs Office. (2013). CORE lab's lighthouse project casts a bright light on IED networks. Monterey, CA: Naval Postgraduate School. Retrieved from http://calhoun.nps.edu/public/bitstream/handle/10945/32340/Naval_Postgraduate_School_-_CORE_Lab%e2%80%99s_Lighthouse_Project_Casts_a_Bright_Light_on_IED_Networks.pdf?sequence=1

Office of the Department of Defense Chief Information Officer. (2012). *Department of Defense mobile device strategy* (Version 2.0). Washington, DC: Department of Defense. Retrieved from: http://www.defense.gov/news/dodmobilitystrategy.pdf

Office of the Department of Defense Chief Information Officer. (2013, November 13). *Field Information Support Tool – Global Information Grid Waiver Requirement* [Memorandum]. Washington, DC: The Pentagon.

O'Neill, P., & Sohal, A. S. (1999). Business process reengineering: A review of recent literature. *Technovation, 19*, 571–581.

Patnaik, D., & Mortensen, P. (2009). Wired to care: How companies prosper when they create widespread empathy. San Mateo, CA: FT Press, 2009.

Privacy Rights Clearinghouse. (2013). Privacy in the age of the smartphone. Retrieved from http://www.privacyrights.org/fs/fs2b-cellprivacy.htm#5

PR Newswire Association. (2011). Lockheed Martin provides affordable smartphone tactical network capability to U.S. Marine Corps. Retrieved from

http://www.thefreelibrary.com/Lockheed+Martin+Provides+Affordable+Smartphone+Tactical+Network...-a0271902814

Reddy, P. (2012). *AFCEA Quantico-Potomac chapter*. [PowerPoint presentation] Retrieved from: http://www.afcea-qp.org/wp-content/uploads/2012/12/MC3_AFCEA_OVERVIEW_NOV_2012_v3.pdf

Roberts N. C., & Longley, C. (2013). "Against all odds: Bottom-up entrepreneurship and innovation in the Department of Defense." In S. P. Osborne & L. Brown (Eds.), *Handbook of Innovation in Public Services* (pp. 176-192). Cheltenham, UK: Edward Elgar Publishing Limited.

Robillard, T. (2011). AMC Social Media Conference provides guidance, best practices for Soldiers, civilians and Families. WWW.ARMY.MIL: The official Homepage of the United States Army. Retrieved from http://www.army.mil/-news/2011/02/10/51643-amc-social-media-conference-provides-guidance-best-practices-for-soldiers-civilians--families/index.html

Sanborn, J. K. (2011, September 7). Marine recruiters receive OK for smartphone camera use. USA Today. Retrieved from http://usatoday30.usatoday.com/news/military/story/2011-09-07/Marine-recruiters-receive-OK-for-smartphone-camera-use/50297466/1

Sauter, D. (2011). Android smartphone relevance to military weather applications. White Sands Missile Range, NM: Army Research Laboratory. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a552755.pdf

Savvion (2006). *Gear up! Savvion process modeler.* Santa Clara, CA: Savvion, Inc. Retrieved from https://cle.nps.edu/access/content/group/432bf46e-e8b1-4979-9abc-45ee99c4e3a7/Course_Documents/Software_Downloads/Savvion_Tutorial/Gear_Up_How_to_Model_in_20_Minutes.pdf

Scarborough, R. (2012a). "Military leaders urgently pushing for new counterterrorism software." *Washington Times*, August 27, 2012.

Scarborough, R. (2012b). "Army gives public relations push to anti-IED system panned by troops." *Washington Times*, October 22, 2012.

Senge, P. M. (1990). *The fifth discipline: The art and practice of the learning organization*. New York: Currency Doubleday.

Seth, A., & Keshav, S. (2005). Practical security for disconnected nodes. In *1st IEEE ICNP Workshop on Secure Network Protocols* (pp. 31–36). Boston, MA: IEEE.

Simental, A. (2010). Smartphones, smart soldiers. *NCO Journal*, *19*(12), 20-23.

Simpson, M. T., Backman, K., & Corley, J. (2011). *Hands-On Ethical Hacking and Network Defense.* Boston: Course Technology, Cengage Learning.

Smith, A. (1956). *An inquiry into the nature and causes of the wealth of nations*. Ed., C.J. Bullock New York: PI Collier & Son.

Stewart, T. A. (1997). Intellectual capital: The new wealth of organizations. New York: Doubleday.

Tapscott, D., & Williams, A. D. (2012). *Macrowikinomics: New solutions for a connected planet.* New York: Portfolio/Penguin.

U.S. Army Office of the Chief of Public Affairs (2011). Social media roundup, geotags and location-based social networking applications. OPSEC briefing. Retrieved from http://dmna.state.ny.us/members/geotagging.pdf

U.S. Army Office of the Chief of Public Affairs. (2012). *U.S. Army social media handbook*. Washington, DC: U.S. Department of the Army. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a563871.pdf

U.S. Department of Defense (2014a). DOD Issuances Website: Processing DOD issuances. Retrieved from http://www.dtic.mil/whs/directives/corres/writing/DOD_process_home.html

U.S. Department of Defense. (2014b). Instruction 8500.01: Cybersecurity. Washington, DC: DOD CIO. Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf

U.S. Department of Defense. (2014c). Instruction 8510.01: Risk management framework for DOD information technology. Washington, DC: DOD CIO. Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf

U.S. Department of Defense. (2013a). Instruction 5025.01: DOD Directives Program. Washington, DC: Director of Administration and Management. Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/502501p.pdf

U.S. Department of Defense. (2013b). Instruction 8320.02: Sharing data, information, and information technology services in the Department of Defense. Washington, DC: DOD CIO. Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/832002p.pdf

U.S. Department of Defense. (2011). Instruction 8520.02: Public key infrastructure and public key enabling. Washington, DC: ASD (NII)/DOD CIO. Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/852002p.pdf

U.S. Department of Defense. (2009a). Directive 8100.04: DOD Unified Capabilities. Washington, DC: ASD (NII)/DOD CIO. Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/810004p.pdf

U.S. Department of Defense. (2009b). Directive 8000.01: Management of the Department of Defense Information Enterprise. Washington, DC: ASD (NII)/DOD CIO. Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/800001p.pdf

U.S. Department of Defense. (2004). Directive 8100.02: Use of commercial wireless devices, services, and technologies in the Department of Defense global information grid. Washington, DC: ASD (NII). Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/810002p.pdf

U.S. Marine Corps. (1996). *Command and Control* (MCDP-6). Washington, DC: Headquarters Marine Corps. Retrieved from FAS website: http://www.fas.org/irp/dodir/usmc/,cdp6.pdf

U.S. Marine Corps. (2010a). *35th Commandant of the Marine Corps planning guidance* (PCN 50100700000). Washington, DC: Author. Retrieved from: http://www.hqmc.marines.mil/Portals/142/Docs/CMC%2035%20Planning%20Guidance%20FINAL%5B1%5D.pdf

U.S. Marine Corps. (2010b). *Vision and strategy for 2025* (PCN 50100654800). Washington, DC: USMC. Retrieved from: http://www.onr.navy.mil/~/media/Files/About-ONR/usmc_vision_strategy_2025_0809.ashx

VanAssche, J. R. (2014). Comprehensive security analysis of field information support tool architecture and applications (Master's Thesis).

Varadharajan, V. (2000). Security enhanced mobile agents. In *Proceedings of the 7th ACM conference on Computer and communications security* (pp. 200–209). New York: ACM.

Whittaker, L. (2011). *Broadband cellular 4G and beyond* [White Paper]. Suffolk, Virginia: Command, Control, Communications and Computers Assessment Division (C4AD), U.S. Army.

Zefferer, T., Kreuzhuber, S., & Teufl, P. (2013). Assessing the suitability of current smarthphone platforms for mobile government: Lecture notes in computer science. In A. Kő, C. Leitner, Leitold, & A. Prosser, *Technology-Enabled Innovation for Democracy, Government and Governance* (pp. 125–139). Berlin, Germany: Springer.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California